Union Calendar No. 482

107TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPORT
107–767

DEFENSE SECURITY SERVICE: THE PERSONNEL SECURITY INVESTIGATIONS [PSI] BACKLOG POSES A THREAT TO NATIONAL SECURITY

SIXTH REPORT

BY THE

COMMITTEE ON GOVERNMENT REFORM

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

OCTOBER 24, 2002.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

U.S. GOVERNMENT PRINTING OFFICE

82–235 PDF WASHINGTON : 2002

COMMITTEE ON GOVERNMENT REFORM

DAN BURTON, Indiana, *Chairman*

BENJAMIN A. GILMAN, New York
CONSTANCE A. MORELLA, Maryland
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEPHEN HORN, California
JOHN L. MICA, Florida
THOMAS M. DAVIS, Virginia
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
BOB BARR, Georgia
DAN MILLER, Florida
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
JOHN SULLIVAN, Oklahoma

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
PATSY T. MINK, Hawaii
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, Washington, DC
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
ROD R. BLAGOJEVICH, Illinois
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
JIM TURNER, Texas
THOMAS H. ALLEN, Maine
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

BERNARD SANDERS, Vermont
(Independent)

KEVIN BINGER, *Staff Director*
DANIEL R. MOLL, *Deputy Staff Director*
JAMES C. WILSON, *Chief Counsel*
ROBERT A. BRIGGS, *Chief Clerk*
PHIL SCHILIRO, *Minority Staff Director*

SUBCOMMITTEE ON NATIONAL SECURITY, VETERANS AFFAIRS AND INTERNATIONAL RELATIONS

CHRISTOPHER SHAYS, Connecticut, *Chairman*

ADAM H. PUTNAM, Florida
BENJAMIN A. GILMAN, New York
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
STEVEN C. LATOURETTE, Ohio
RON LEWIS, Kentucky
TODD RUSSELL PLATTS, Pennsylvania
DAVE WELDON, Florida
C.L. "BUTCH" OTTER, Idaho
EDWARD L. SCHROCK, Virginia

DENNIS J. KUCINICH, Ohio
BERNARD SANDERS, Vermont
THOMAS H. ALLEN, Maine
TOM LANTOS, California
JOHN F. TIERNEY, Massachusetts
JANICE D. SCHAKOWSKY, Illinois
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

DAN BURTON, Indiana

HENRY A. WAXMAN, California

LAWRENCE J. HALLORAN, *Staff Director and Counsel*
J. VINCENT CHASE, *Chief Investigator*
JASON CHUNG, *Clerk*
DAVID RAPALLO, *Minority Counsel*

LETTER OF TRANSMITTAL

HOUSE OF REPRESENTATIVES,
Washington, DC, October 24, 2002.

Hon. J. DENNIS HASTERT,
Speaker of the House of Representatives,
Washington, DC.

DEAR MR. SPEAKER: By direction of the Committee on Government Reform, I submit herewith the committee's sixth report to the 107th Congress. The committee's report is based on a study conducted by its Subcommittee on National Security, Veterans Affairs and International Relations.

DAN BURTON,
Chairman.

CONTENTS

Union Calendar No. 482

107TH CONGRESS, *2d Session* } HOUSE OF REPRESENTATIVES { REPORT 107–767

DEFENSE SECURITY SERVICE: THE PERSONNEL SECURITY INVESTIGATIONS [PSI] BACKLOG POSES A THREAT TO NATIONAL SECURITY

OCTOBER 24, 2002.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

---

Mr. BURTON, from the Committee on Government Reform submitted the following

SIXTH REPORT

On October 9, 2002, the Committee on Government Reform approved and adopted a report entitled "Defense Security Service: the Personnel Security Investigations [PSI] Backlog Poses a Threat to National Security." The chairman was directed to transmit a copy to the Speaker of the House.

I. SUMMARY

The Government Reform Committee, National Security, Veterans Affairs and International Relations [NSVAIR] Subcommittee conducted an oversight investigation of the Defense Security Service. The subcommittee examined the agency's personnel security investigation [PSI] program to determine the reasons behind a growing PSI backlog. Personnel security investigations are conducted to determine whether an individual should be granted access to classified information. This is a critical first step in safeguarding the Nation's secrets.

Findings:

1. The Defense Security Service cannot accurately determine the size or forecast the elimination of the personnel security investigations backlog.
2. There was a lack of management oversight of the Defense Security Service by the Department of Defense [DOD] that contributed to a backlog of personnel security investigations.

3. Acquisition of the Case Control Management System [CCMS] and the Joint Personnel Adjudication System [JPAS] did not comply with the requirements of the Clinger-Cohen Act and may not provide effective caseload management.
4. There are no common standards for investigating and adjudicating a personnel security clearance in a timely manner.
5. Defense Security Service and the Office of Personnel Management [OPM] personnel security clearance investigators have difficulty accessing State and local criminal history record information [CHRI].

Recommendations:

1. The Secretary of Defense should continue to report the personnel security investigations program including the adjudicative process as a material weakness under the Federal Managers' Financial Integrity Act to ensure needed oversight is provided to effectively manage and monitor the personnel security process from start to finish.
2. The Secretary of Defense should set priorities and control the flow of personnel security investigation requests for all DOD components.
3. The Secretary of Defense should closely monitor the interface between JPAS and CCMS to ensure effective management of investigative and adjudicative cases and avoid further backlogs.
4. The National Security Council should promulgate Federal standards for investigating and adjudicating personnel security clearances in a timely manner.
5. The Secretary of Defense and the Attorney General jointly should develop a system which allows DSS and OPM investigators access to State and local criminal history information records [CHIR].

II. BACKGROUND

Acts of espionage have had serious consequences for the United States, military personnel and citizens. To prevent acts of espionage, and to ensure the interests of the United States are protected requires certain information concerning national security be protected against unauthorized disclosure. Information may not be classified unless its unauthorized disclosure reasonably could be expected to cause damage to national security. The degree of expected damage from unauthorized release determines which of the three levels of classification will be applied: TOP SECRET—"exceptionally grave damage" to the national security; SECRET—"serious damage" to the national security; and, CONFIDENTIAL—"damage" to the national security.[1]

Each year thousands of classified programs and projects are carried out by the U.S. Government. These activities generate millions of items of classified documents and information used by the mili-

[1] Executive Order No. 12356 of Apr. 2, 1982, *National Security Information Guidelines*, Sec. 1.1, *Classification Levels,* Code of Federal Regulations, Office of the Federal Register National Archives and Records Administration.

tary, civilian and contract employees. This classified information is not only in the form of documents. An enormous inventory of classified equipment and components must be safeguarded. Increasingly, classified data is being processed, transmitted and stored electronically, posing serious new problems of protection.

The Department of Defense through the Defense Security Service conducts personnel security investigations [PSI] to determine whether an applicant should be granted access to classified information. Upon completion of the PSI by DSS, the information collected is sent to one of eight adjudication facilities for security clearance determination.[2]

At the end of fiscal year 2001 DSS reported, 2,127,476 active duty military, civilian, and contractor employees held personnel security clearances: 62,108 employees held confidential clearances, 1,607,727 employees held secret clearances, 209,897 held top secret, and 247,744 held top secret/SCI clearances. On average, an initial top-secret investigation takes DSS approximately 521 days to complete and the Office of Policy and Management approximately 108 days to complete and costs approximately $2,400 per investigation for DSS and approximately $2,775 per investigation for OPM.[3]

The Department of Defense is requesting $443.0 million for DSS operations for fiscal year 2003 a decrease of $51.3 million over fiscal year 2002.[4] The investigation budget for DSS and OPM is $269.7 million and $157.4 million respectively.[5] Despite the overall reduction, DOD is requesting an additional $3.6 million for case control management system improvements in fiscal year 2003 and increase of 29 percent over fiscal year 2002.[6]

Three primary business areas comprise the DSS mission: No. 1, the Personnel Security Investigations Program, the investigations conducted under this program are used by the DOD adjudication facilities to determine an individual's suitability to enter the armed forces, to access classified information, or to hold a sensitive position within the Department of Defense; No. 2, the National Industrial Security Program [NISP] established by Executive Order 12829,[7] which primarily ensures private industry, colleges, and universities that perform government contracts or research safeguard classified information in their possession; and No. 3, the Security Training and Education Program, which provides security education and training programs to support DSS components, DOD agencies, military departments and contractors.[8]

---

[2] Executive Order No. 12968 of Aug. 2, 1995, *Access to Classified Information, Sec. 1.2, Access to Classified Information,* Code of Federal Regulations, Office of the Federal Register National Archives and Records Administration.

[3] Email from Lt. Colonel Leo Clark, Office of the Secretary of Defense, Subject: DSS Final Report, Feb. 15, 2002, (in subcommittee files).

[4] Defense Security Service, Fiscal Year 2003 Budget Estimates, February 2002, Exhibit Fund-14 Revenue and Expenses, (in subcommittee files).

[5] See supra note 3.

[6] Defense Security Service, Fiscal Year 2003 Budget Estimates, February 2002, Exhibit Fund-9a, Activity Group Capitol Investment Summary, (in subcommittee files).

[7] Executive Order No. 12829 of Jan. 6, 1993, *National Industrial Security Program,* Code of Federal Regulations, Office of the Federal Register National Archives and Records Administration.

[8] Defense Security Service, FY2003 Amended Budget Submission, February 2002, p. DSS–2, (in subcommittee files).

In addition, DSS supports counterintelligence, operation and maintenance, and research and development activities of the Department of Defense Polygraph Institute [DODPI].[9] DODPI is an educational, research and policy-establishing institute for the forensic discipline of psychophysiological detection of deception. The Defense Security Service is under the direction, authority, and control of the Office Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (OASD–C3I) in accordance with the provisions of DOD Directive 5105.42.[10]

Top secret, secret, and confidential clearances require reinvestigation every 5, 10, and 15 years, respectively. The importance of reinvestigating and reevaluating a personnel security clearance is as much a matter of national security as the original background check. According to GAO, failure to have an up-to-date security clearance would pose a threat to national security.[11]

DSS conducts personnel security background investigations within the 50 States, the District of Columbia, the Commonwealth of Puerto Rico, and the trust territories. DSS requests the military departments and other U.S. Government agencies, as appropriate, to complete investigative leads in areas not set forth above.[12]

A Defense Security Service personnel security investigation [PSI] is intended to determine an individual's loyalty to the United States, character, trustworthiness, honesty, reliability, discretion, and judgment are such that the person can be expected to comply with government policy and procedures for safeguarding classified information.[13]

In 1994, the Joint Security Commission determined "national security policy was fragmented and lacked an effective mechanism to ensure commonality. Multiple groups with differing interests and authorities worked independently of one another with insufficient integration of security policy and procedures."[14] Because of this fragmentation of security policy and structure, the President established the Security Policy Board to consider, coordinate, and recommend policy directives for national security. The Security Policy Board was the principal mechanism for reviewing and proposing to the National Security Council [NSC] legislative initiatives and Executive orders pertaining to security policy, procedures and practices that do not fall under the statutory jurisdiction of the Secretary of State.[15] [16]

In August 1995, under Executive Order 12968, "Access to Classified Information," the President directed the Board to develop a set of uniform investigative standards and adjudicative guidelines for

---

[9] Ibid., p. DSS–11.

[10] Department of Defense, Directive No. 5105.42, Subject: Defense Security Service [DSS], May 13, 1999, (in subcommittee files).

[11] Testimony of Carol R. Schuster, Associate Director, U.S. General Accounting Office, NSVAIR Subcommittee hearing, Serial No. 106–267, p. 38.

[12] Defense Security Service, Personnel Security Investigation Manual, revised Oct. 15, 1999, 1–329. DSS PSI Mission, pp. 6–7, (in subcommittee files).

[13] See supra note 2, Sec. 3.1.

[14] *Redefining Security: A Report to the Secretary of Defense and the Director of Central Intelligence,* p. 2, Feb. 28, 1994, Joint Security Commission, Washington, DC 20505.

[15] Security Policy Board Mission Statement (in subcommittee files).

[16] The Bush administration transferred the duties assigned to the Security Policy Board to NSC Policy Coordination Committees pursuant to Presidential Directive, NSPD–1, *Organization of the National Security Council System,* Feb. 13, 2001, (in subcommittee files).

determining eligibility for access to classified information.[17] In 1997, the Security Policy Board issued standard procedures to govern the access to classified information.[18] The investigative standards developed by the Security Policy Board include examination of:

- Birth and citizenship records;
- Corroboration of education;
- Verification of employment for the past 7 years and interviews with supervisors and co-workers:
- Interviews with character references with social knowledge of the subject;
- Neighborhood checks and interviews with neighbors to confirm all residences for the past 3 years;
- National agency checks including the FBI and CIA;
- Financial review including a credit bureau check;
- Local agency check of criminal history records and other public records to verify any civil or criminal court actions involving the individual; and
- A personal interview with the individual.

The objectives of the investigative standards are to (1) examine and assess various aspects of an individual's trustworthiness and reliability, taking into account both positive and negative issues and (2) bring some uniformity and consistency to Federal processes to avoid unnecessary and costly reinvestigations when an individual switches agencies.[19]

The standards for reinvestigations are essentially the same as those for initial investigations, with two exceptions. Reinvestigations do not require corroboration of proof of birth and citizenship, and education. The basis for not requiring this information for reinvestigation cases is that it is obtained in the initial investigation, and does not change.[20]

The process of obtaining a security clearance begins with a request from a military commander, contractor, or other DOD official for a security clearance for an individual because of the sensitive nature of his or her duties. The individual completes the appropriate personnel security form for the level of classification needed—CONFIDENTIAL, SECRET, or TOP SECRET.[21] The Personnel Security form requires the candidate for a security clearance to provide personal background information needed to conduct the personnel security investigation. The questionnaire is then forwarded to the Defense Security Service's Operations Center.

Defense Security Service analysts review clearance requests to ensure all necessary forms are complete, develop a scope for the investigation, and assign the required work to 1 or more of the 12 DSS field-operating locations throughout the United States. An investigation may be sent to one or more operating locations depending on where the individual seeking clearance has lived, worked, or attended school. Once received in the field, an investigation is assigned to an investigator who seeks information in that geographic

---

[17] See supra note 2.

[18] Security Policy Board, *Investigative Standards for Background Investigations for Access to Classified Information,* SPB Issuance 1–97, Mar. 24, 1997, (in subcommittee files).

[19] See supra note 2, Sec. 2.4.

[20] Ibid.

[21] See supra note 12, Sec. 4, pp. 14–15.

location about the individual's loyalty, character, reliability, trustworthiness, honesty, and financial responsibility.

As the investigation elements are completed, the field sends reports to the DSS Operations Center, where case analysts determine if all investigative criteria have been met and all issues relevant for a clearance decision have been resolved. DSS sends the completed investigation to one of eight adjudication facilities for security clearance determination.

The Army, Navy, Air Force, the National Security Agency [NSA], the Defense Intelligence Agency [DIA], the Defense Office of Hearings and Appeals [DOHA], the Joint Chiefs of Staff [JCS], and the Washington Headquarters Service [WHS] operate the eight adjudication facilities.

The adjudicative process is an examination of a sufficient period of the applicant's life to determine if the person is an acceptable security risk.[22] The adjudication process is the weighing of a number of variables known as the "whole person concept."[23] The whole person concept is the consideration by the adjudicator of all available, reliable information about the person, past and present, favorable and unfavorable, when reaching a determination. In deciding if a clearance should be granted or denied, the adjudication facility staffs base their decision on the following adjudicative factors:[24]

- Allegiance to the United States;
- Foreign influence;
- Sexual behavior;
- Personal conduct;
- Financial consideration;
- Alcohol consumption and drug involvement;
- Emotional, mental, and personality disorders;
- Criminal conduct;
- Security violations;
- Outside activities; and
- Misuse of information technology

The ultimate determination of whether the granting or continuing of eligibility for a security clearance must be clearly consistent with the interests of national security based upon careful consideration of the adjudication factors, each of which is to be evaluated in the context of the "whole person."[25]

Since 1985, blue ribbon commissions[26] and the General Accounting Office [GAO], have recommended the quality, timeliness and frequency of personnel security background investigations be improved.[27]

More recently, management deficiencies identified by GAO and the DOD–OIG included the failure of the Defense Security Service, formerly known as the Defense Investigative Service, to provide ac-

---

[22] Security Policy Board, *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information,* SPB Issuance 2–97, Mar. 24, 1997, (in subcommittee files).

[23] See supra note 12, Sec. 4, p. 18.

[24] Ibid., p. 17.

[25] Department of Defense, *Adjudicative Guidelines for Determining Eligibility for Access to Classified Information,* DOD 5200.2–R, (in subcommittee files).

[26] *Keeping the Nation's Secrets: A Report to the Secretary of Defense by the Commission to Review DOD Security Policies and Practices,* Nov. 19, 1985, DOD Security Commission, Office of the Secretary of Defense, Washington, DC 20301, (in subcommittee files).

[27] *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks,* (GAO/NSIAD–00–12) in October 1999.

curate and timely personnel security investigations, inattention to personnel training, and the acquisition and installation of new information technology systems without the benefit of risk assessment, proper testing or backup.[28]

According to the 1994 Joint Security Commission Report, delays in the investigative and adjudicative process contribute directly to government costs.[29] As far back as 1981, the General Accounting Office reported to Congress nearly $1 billion was wasted annually because of investigative backlogs at the Defense Security Service.[30]

The subcommittee conducted three Defense Security Service oversight hearings: on February 16, 2000,[31] September 20, 2000,[32] and March 2, 2001.[33] The purpose of the hearings was to examine performance and management challenges confronting DSS, particularly the agency's plans to address the personnel security investigations backlog and the extent to which the automated case control management system can be improved to address the backlog of security clearances.

The backlog was a result in large part due to lax OASD–C3I oversight, DSS mismanagement, CCMS malfunctions, and OASD–C3I and DSS's inability to keep pace with changing personnel security clearance criteria and Presidential directives.

Hearing testimony offered optimistic views for determining the size and timetables for the elimination of the personnel security investigations backlog[34] and "dramatic improvements"[35] in the case control management system despite recommendations to replace the system.[36]

Based on the testimony and documentary record, the subcommittee concludes lax oversight of DSS by the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD–C3I) contributed directly to the degradation of DSS productivity and effectiveness.[37]

Proactive intervention by OASD (C3I) did not occur until October 1999, after the backlog had attained crisis proportions.[38] Only after

---

[28] Department of Defense, Office of Inspector General Audit Report, *Program Management of the Defense Security Service Case Control Management System,* Report No. D–2001–019, Dec. 15, 2001.

[29] See supra note 14, p. 47.

[30] Ibid.

[31] *Defense Security Service Oversight Hearing,* 106th Cong., 2d sess., (2000) National Security, Veterans Affairs, and International Relations [NSVAIR] Subcommittee hearing, Feb. 16, 2000, Serial No. 106–152.

[32] *Oversight of the Defense Security Service: How Big is the Backlog of Personnel Security Investigations?,* 106th Cong., 2d sess., (2000) National Security, Veterans Affairs, and International Relations [NSVAIR] Subcommittee hearing, Sept. 20, 2000, Serial No. 106–267.

[33] *Defense Security Service: Mission Degradation?,* 107th Cong., 1st sess., (2001) National Security, Veterans Affairs and International Relations [NSVAIR] Subcommittee hearing, Mar. 2, 2001, Serial No. 107–40.

[34] Testimony of Lt. General Charles J. Cunningham Jr., USAF (Ret), Director-Defense Security Service, National Security, Veterans Affairs, and International Relations [NSVAIR] Subcommittee hearing, Feb. 16, 2000, Serial No. 106–152, p. 114.

[35] Statement of Lt. General Charles J. Cunningham Jr., USAF (Ret), Director-Defense Security Service, National Security, Veterans Affairs and International Relations [NSVAIR] Subcommittee hearing, Sept. 20, 2000, Serial No. 106–267, p. 75.

[36] TRW's Evaluation of DSS CCMS, Final Report, July 21, 1999, Contract No: DASW01–99–F–3060–P001, June 22, 1999, (in subcommittee files).

[37] *An Assessment of the Department of Defense Personnel Security Program: A Report to the Deputy Secretary of Defense,* Personnel Security Investigations Process Review Team, Oct. 31, 2000, (in subcommittee files).

[38] Ibid., p. 44.

much criticism and scrutiny from Congress,[39] the media,[40] other government agencies,[41] and defense contractors[42] did the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [C3I] request a serious review of the status and options regarding the personnel security investigations backlog.

The review produced an internal report issued February 8, 2001 entitled *Personnel Security Investigations: Mission Degradation!*[43] This report called for "bold action"[44] and contained worse news, and more sweeping recommendations, than the Assistant Secretary anticipated. The report shows that the time to complete personnel security investigations upon which clearances are based is getting longer. As the time to complete investigations has grown, the number of investigations pending is also growing. In December 2000, output exceeded input for the first time, but it remains to be seen whether this constitutes a trend or a one-time improvement.

Between June 9, 1999 and February 8, 2001,[45] memoranda, program initiatives, and policy directives to eliminate the PSI backlog resulted in little improvement to provide timely investigations and clearances to soldiers, sailors, airmen, Marines, DOD civilian and defense contractors.

As a result, defense contractors are losing qualified new hires that cannot wait almost a year for DSS to complete an initial investigation.[46] In addition, defense contractors have found themselves unable to perform billions of dollars of work because employees have not obtained routine clearances. These delays threaten to affect some facilities' ability to effectively perform on defense contracts and meet cost schedules. A survey conducted by the Aerospace Industries Association revealed, as of December 2000, 12 percent of the secret clearance requests were pending for more than 1 year and 30.6 percent of the top secret clearance requests were pending for more than 1 year. Another survey conducted in November 1999 revealed it cost the aerospace industry an estimated $149.9 million for clearances more than 90 days old.[47]

In 1997, the DOD Office of Inspector General reported, the Director of the Defense Security Service had designated DSS as a "reinvention laboratory" to assess the agency's policies and procedures in an effort to determine their relevance and responsiveness to the

---

[39] The General Accounting Office [GAO] reviewed DOD's personnel security investigative functions at the request of Congressman Ike Skelton, ranking member, House Committee on Armed Services. GAO issued the report *DOD Personnel: Inadequate Personnel Security Investigations Pose National Security Risks,* (GAO/NSIAD–00–12) in October 1999.

[40] USA Today, *Pentagon Crisis: Security Check Backlog,* Edward T. Pound, June 3, 1999, (in subcommittee files).

[41] Memorandum: *Investigation Standards for Access to Classified Information,* Oct. 26, 1996, from Peter D. Saderholm, Director-Security Policy Board to Richard J. Wilhelm, et. al., Co-Chair, Security Policy Forum, (in subcommittee files).

[42] Aerospace Industries Association, 1250 Eye Street NW., Suite 1200, Washington, DC 20005, *Background Investigation Timeliness Tracking Survey,* December 2000, (in subcommittee files).

[43] *Personnel Security Investigations: Mission Degradation!* OASD (C3I) Security Directorate Draft Report for Comment, Richard F. Williams, Director of Security, Feb. 8, 2001, (in subcommittee files).

[44] Ibid., p. 1.

[45] Ibid., p. 21–24.

[46] See supra note 42.

[47] Aerospace Industries Association, 1250 Eye Street NW., Suite 1200, Washington, DC 20005, *DSS Clearance Backlog Summary,* November 1999, (in subcommittee files).

users of DSS services.[48] Under this "reinventing government" initiative, DSS management and employees reviewed the investigation process to identify ways to improve the quality and timeliness of investigations.[49] Initiatives developed by DSS managers included:

- reorganizing and streamlining the agency,
- becoming a performance based organization [PBO],
- implementing new investigative procedures to improve the timeliness of investigations,
- automating the scope development and review of investigations, and
- charging a fee for service.[50]

The following year, the Department of Defense Office of the Inspector General (DOD–IG) conducted an audit of DSS to determine the effectiveness and efficiency of the management of the personnel security program. Specifically, the DOD–IG reviewed the processes for conducting and the procedures for disseminating information related to personnel security investigations [PSI].[51]

Although, at the time, the audit conducted by the Department of Defense-Office of the Inspector General "strongly supported" Defense Security Service reinvention efforts,[52] GAO found DSS's initiative exacerbated the problem of accurate and timely personnel security investigations contributing to a massive backlog of PSI cases.[53]

The backlog of PSI cases can be attributed to a number of factors. In his memorandum of June 15, 2000, the Assistant Secretary of Defense (C3I) wrote, "the periodic reinvestigation [PR] backlog has reached significant proportions largely as a result of the PR quota that was imposed from FY96 to present by this office as well as the implementation of new national policy which lowered the interval for SECRET PR's from 15 to 10 years and set a new 15 year PR requirement for CONFIDENTIAL PR's." [54]

In 1995, the Assistant Secretary of Defense (C3I) directed DOD components to cease submitting periodic reinvestigation [PR] requests that were due to DSS,[55] and then in June 1996, the Assistant Secretary of Defense (C3I) revised this directive and established a quota system allowing DOD components to submit up to 40,000 secret and 42,000 top secret PR requests per year.[56] Although these directives were intended to reduce the turnaround time to process PSI cases, the directives created a backlog and a pent-up demand for security clearances. In addition, at that time, the Assistant Secretary announced that DOD would adopt new investigative standards.[57] These standards provided less complete information for use by adjudicators in determining whether to grant

---

[48] Department of Defense, Office of Inspector General, Audit Report No. 97–196, *Personnel Security in the Department of Defense,* p. 17, July 25, 1997 (in subcommittee files).
[49] Ibid., p. 5.
[50] Ibid.
[51] Ibid., Executive Summary.
[52] Ibid., p. 12.
[53] See supra note 27.
[54] Memorandum: *Personnel Security Investigations Backlog,* June 15, 1999, from Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Arthur L. Money to Secretaries of the Military Departments, et. al., (in subcommittee files).
[55] See supra note 27, p. 30.
[56] Ibid.
[57] Ibid., p. 19.

clearances, which further delayed the security clearance process. And, finally there were system failures of the newly deployed automated case control management system for tracking and processing PSI cases.[58] All of these factors: the PR quota system; new investigative standards; and CCMS failures all affected DOD's capacity to process PSI cases and contributed to the backlog.

According to Carol Schuster of the General Accounting Office, "Since 1998, various DOD documents and statements have cited several widely divergent backlog estimates ranging from about 452,000 to 992,000."[59] The backlog was a result, in part, of internal procedure changes in DSS. According to the General Accounting Office, DSS officials stated that once the agency became a reinvention laboratory, it was allowed to operate, for the most part, at its own discretion with little or no oversight from the Assistant Secretary of Defense-Command, Control, Communications and Intelligence (ASD–C3I).[60]

Knowing the accurate size of the backlog is an important step toward effectively managing and eliminating the backlog. In 1999 DSS attempted to determine the size of the PSI case backlog. The MITRE Economic and Decision Analysis Center was hired to work with DSS to conduct an analysis of the backlog through the use of formal statistical sampling and manual counts.[61] MITRE reported in 2000, with 95 percent confidence, the true size of the backlog population falls between 206,107 and 558,552 cases.[62]

In October 1998, to expedite PSI case processing, the Defense Security Service acquired and deployed a new information technology system referred to as the Case Control Management System at a cost of $100 million.[63] The stated goals of CCMS were to simplify the investigative process by eliminating unnecessary manual activity, and automate the processes associated with the overall management of PSI cases.[64] CCMS was supposed to expedite PSI case processing by linking all relevant information critical to an investigation through a network of DSS subsystems.[65] PSI case processing includes the collection, tracking, adjudication, and disseminating of information about security clearances for more than 15 million individuals. The CCMS network is primarily located at the DSS Personnel Investigations Center in Fort Meade, MD.

In 1999, assessments of the case control management system were conducted by TRW[66] and a DOD Red Team.[67] Those assessments found deficiencies in acquisition strategy, program management, system integration, and operations and maintenance. It was estimated that an additional $87.2 million to $103 million would be

---

[58] Ibid., p. 26–28.
[59] Statement of Carol R. Schuster, Associate Director, U.S. General Accounting Office, NSVAIR Subcommittee hearing, Serial No. 106–267, p. 8.
[60] See supra note 27, p. 19.
[61] Mitre Technical Report, *The Defense Security Services Backlog of Periodic Reinvestigations: Statistical Analysis and Risk Prioritization Procedure,* p. iii–iv, February 2000, Paul R. Garvey, et. al., (in subcommittee files).
[62] Ibid., p. v.
[63] General Accounting Office briefing for the House Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations [NSVAIR], briefing slide, p. 30, Nov. 8, 1999, (in subcommittee files).
[64] See supra note 48, p. 9.
[65] See supra note 63.
[66] See supra note 36.
[67] DOD Red Team Advanced Draft, Red Team Recommendations—Transition Ahead, July 14, 1999.

needed fiscal year 1999–2006 to address the deficiencies for a system that was projected to cost $100 million when fully operational.[68]

According to GAO, the case control management system suffers serious weaknesses and will be far more difficult to fix than DSS anticipates. During the September 2000 NSVAIR Subcommittee hearing, addressing the CCMS issue, the Director of DSS stated, "there were dramatic improvements resulting from the software enhancements and corrections that have been implemented within the last 6 months."[69] Yet the DOD–IG in December 2000 recommended the Assistant Secretary of Defense-C3I analyze whether the investment for the Case Control Management System provides the best business solution when compared to alternative solutions for opening, tracking, and closing personnel investigation cases.

The Defense Security Service is making progress since the subcommittee's oversight investigation of the agency began a little more than 2 years ago. However, DSS has a long way to go to resolve systemic problems of tracking and promptly completing personnel security investigations. In the meantime, national security risks increase and the need for additional financial resources grows.

According to Donald Mancuso, Acting Inspector General, "Simply put, the inability to track and promptly complete personnel security investigations has had a devastating effect on the Department's ability to ensure that national security is protected and that military, civilian and contractor employees have the timely clearances needed to complete their jobs. On a human level, the lack of timely clearances prevents people from obtaining employment in DOD, and in the case of contractor employees, causes the loss of hundreds of millions of tax dollars paid to contractors or for employees awaiting clearances."[70]

III. Discussion

FINDINGS

1. The Defense Security Service cannot accurately determine the size or forecast the elimination of the personnel security investigations backlog.

The Defense Security Service has a personnel security investigation backlog that has ranged from approximately 350,000 to 900,000 cases. The disparity in the range is a result of different methodologies used to count the backlog, efforts to prioritize the most sensitive personnel security investigations, and the elimination of cases as a result of changes in employment status for the individual needing a security clearance. Priorities for investigations by category include presidential support, sensitive compartmented information [SCI], and special access programs [SAPs] which impose need-to-know or access controls beyond those normally pro-

[68] See supra note 36, Sec. 7, p. 67–68.
[69] See supra note 35, p. 75.
[70] Testimony of Donald Mancuso, Acting Inspector General, Office of the Inspector General, Department of Defense, NSVAIR Subcommittee hearing, Serial No. 106–267, p. 38.

vided for access to confidential, secret, or top secret information.[71] The inability to prioritize investigations has resulted in extensive delays in clearances for some high priority projects.[72] Additionally, there is currently no automated method for notifying DSS of a priority investigation. The requester has to notify DSS when a priority investigation is provided and special processing is necessary. DSS manually pulls the request and moves the investigation case to the front of the queue.[73] It is currently taking, on average, more than a year to complete a personnel security reinvestigation for someone needing a top-secret clearance.

Testifying before the NSVAIR Subcommittee, GAO's Carol Schuster, Associate Director for National Security Issues stated, "There were several reasons that led to this backlog. The implementation of a quota system on the number of PSI requests that could be submitted created a pent-up demand contributing to the backlog. Then we had new requirements[74] that were instituted during this period for re-investigations on secret and confidential clearances. Those had not been requirements before. So this added to the backlog. Also, the automated case control management system that we were talking about just did not work. CCMS system failures contributed to the backlog."[75]

Carol Schuster stated DSS also pointed to additional factors contributing to the backlog, "One is that they feel that there are more people requesting clearances because of the growing number of information technology jobs that may require clearances, and the reduction of DSS staff and investigators the agency experienced as a result of DOD downsizing. So all of those problems collectively contributed to the problem."[76]

A consultant for DSS reported in February 2000 the effect downsizing had on the Defense Security Service. "As a result of the general downsizing of defense agencies in recent years, DSS staffing has been significantly reduced, dropping from about 4,000 in 1991 to about 2,500 in 1998. In particular, DSS investigators fell from 1,650 to 1,250 during the same period. Meanwhile, the investigative workload for clearances has remained fairly constant over that time."[77]

As congressional[78] and media[79] scrutiny intensified, concerns were raised regarding the growing backlog of personnel security investigations, and the affect the backlog would have on national security. As a result, the NSVAIR subcommittee asked the General Accounting Office to determine how DSS estimates the backlog, as-

---

[71] See supra note 37, p. 19.
[72] Ibid.
[73] Ibid.
[74] Between August 1996 and February 1999, DSS issued 31 policy letters directly related to the manner in which investigations were to be conducted. Several letters announced policy changes that gave investigators greater discretion in how they would meet the standards or pursue issues that might be of significance in deciding to grant clearances. Several of these policies were inconsistent with Federal investigative standards in the requirement to conduct local agency checks of criminal history records, and the verification of public records regarding divorce, bankruptcy, or other court actions, involving the subject.
[75] Testimony of Carol R. Schuster, Associate Director, U.S. General Accounting Office, NSVAIR Subcommittee hearing, Serial No. 106–152, p. 34.
[76] Ibid.
[77] See supra note 61, p. 1.1.
[78] Letter from Congressman Ike Skelton of Missouri to the General Accounting Office a review of DOD's personnel security functions, Mar. 25, 1998.
[79] See supra note 40.

sess the soundness of DOD's backlog estimates, and identify the plans DSS developed to address the backlog problem.

The General Accounting Office reported its findings in August 2000. According to GAO findings, the personnel security reinvestigations backlog for defense, civilian, and contractor personnel was approximately 505,000 reinvestigations, and growing, with an additional 480,000, which had not yet been submitted to DSS from DOD and the military departments. However, the subcommittee learned the actual backlog size was still unknown because existing personnel security databases cannot provide an accurate count of overdue reinvestigations.

"In the absence of a Department-wide database that can accurately measure the reinvestigation backlog, DOD estimates the backlog on an ad-hoc basis, using manual counts and statistical sampling as the primary methods. Using the sampling method, DOD makes a rough and known to be inaccurate estimate from existing personnel security databases." [80]

In that regard, the subcommittee also learned the survey process for determining the backlog was flawed. When the Office of the Secretary of Defense asked Military Departments and Defense agencies to survey their commands and organizations in 1999, they failed to provide the methodology for determining the size of the backlog. As a result, no standard format was used to obtain the figures. Some just filled out the information by using manual counts, while others did a sample survey. A second survey conducted a few months later again did not address methodology. As a result, it appears programs and agencies reported lower numbers giving the erroneous impression that DOD was making progress eliminating the PSI backlog.

From June 9, 1999 to February 8, 2001 the Department of Defense issued 13 policy directives and reports to manage and eliminate the growing backlog of personnel security investigations. These included:

- June 9, 1999—Deputy Secretary of Defense memorandum, *Personnel Security Clearance Investigations Backlog,* directed the elimination of the backlog by September 30, 2000. The memorandum expanded the DOD investigative capacity by shifting a part of the DOD civilian PSI workload to the Office of Policy and Management, directed each military department and defense agency to provide a quarterly plan for eliminating the backlog. The Deputy Secretary further directed that each military department and defense agency to administratively terminate or downgrade all clearances not based on a current investigation or not in process for reinvestigation by September 30, 2000.
- June 15, 1999—Assistant Secretary of Defense (C3I) memorandum, *Personnel Security Clearance Investigations Backlog,* implemented the Deputy Secretary's memorandum of June 9, 1999 by directing a minimum number of additional periodic reinvestigations to OPM for DOD civilian employees and all others to DSS. The Assistant Secretary stressed

[80] *DOD Personnel: More Action Needed to Address Backlog of Security Clearance Reinvestigations,* (GAO/NSIAD–00–215), p. 1–2, U.S. General Accounting Office, in August 2000.

military departments and defense agencies would be expected to identify the resources necessary to fund backlogged of periodic reinvestigation's over and above those already programmed as well as accomplish the adjudications at the backend end of the PSI process.

- September 29, 1999—Assistant Secretary of Defense (C3I) memorandum, *Personnel Security Clearance Investigations,* directed all initial investigations of DOD civilian personnel, except overseas investigations, would be conducted by OPM, and rescinded the June 9, 1999 directive to administratively terminate or downgrade all clearances not based on a current investigation or not in process for reinvestigation by September 30, 2000.
- November 1999—At a meeting of the Defense Management Council, the Deputy Secretary of Defense called for the creation of an Overarching Integrated Process Review Team [OIPT] to find a cure for the PSI backlog problem, and to chart a new path for the future. The Team defined the backlog to be those periodic reinvestigations exceeding the timeframe for which a reinvestigation is required and which has not yet been submitted to the investigative agency.
  The Team asked the military departments to determine their backlog according to the established backlog definition. For DOD agencies and contractors the team used previously developed estimates rather then developing new counts. The Team reported their findings and recommendations in January 2000. The Team determined that the periodic reinvestigation backlog totaled 505,786. The Team recommendations included the transfer of all secret and confidential investigations to OPM and restoration of funding for the Joint Personnel Adjudication System to improve management of the population actually receiving access to the most classified information.
- March 31, 2000—Deputy Secretary of Defense memorandum, *Personnel Security Clearance Investigations Backlog,* directed implementation of the OIPT recommendations and extended the timeline for eliminating the PR backlog to March 31, 2002.
- June 1, 2000—Deputy Secretary of Defense memorandum, *Personnel Security Investigation Process Review,* directed a comprehensive review to baseline the reform of the personnel security process, to establish a "get well" date, and make additional recommendations to expedite the personnel security process effort. A Process Review Team was established to accomplish this effort.
- June 22, 2000—Under Secretary of Defense (Comptroller) memorandum, *Personnel Clearance Backlog and Security Initiatives,* generally referred to as the "Spend Plan," extended the timeline for eliminating the PR backlog to September 30, 2002. The plan provided monthly targets for all DOD components for submitting investigative requests to DSS and OPM, along with the associated funding. PSIs were distributed between DSS and OPM in accordance with

the Deputy Secretary of Defense memorandum dated March 31, 2000.

The plan called for sending 415,841 cases to OPM in fiscal year 2001 and 395,908 in fiscal year 2002. During the same period, DSS was to process 558,619 new cases and 128,000 existing cases in fiscal year 2001; and 388,598 new cases plus 307,000 existing cases in fiscal year 2002. This accounted for all carryover work at DSS and all new work to be submitted over fiscal year 2001 and fiscal year 2002, both backlog cases and the steady-state workload.

In addition, the memorandum call for the appointment of a senior official by each component to monitor processing of personnel security investigations to DSS and OPM, and to establish procedures for monitoring and executing the plan within the component.

- August 22, 2000—Assistant Secretary of Defense (C3I) memorandum, *Personnel Security Clearance Investigations,* implemented the Spend Plan by providing instructions to the components for submitting investigative requests including quarterly progress reports. To ensure success, the military departments and defense agencies were required to appoint a senior official to monitor the processing of investigations to DSS and OPM and encouraged to have their Inspectors General include compliance as a matter of interest during inspections for fiscal year 2001 and fiscal year 2002.
- September 11, 2000—Deputy Secretary of Defense memorandum, *Personnel Security Investigation Process Review,* directed all military departments and defense agencies to conduct a periodic reinvestigation survey because the backlog baseline may have changed considerably due to a lapse of time and the efforts of the Departments in submitting PR requests.
- October 11, 2000—The report, *An Assessment of DOD's Plan to Eliminate the Periodic Reinvestigation [PR] Backlog,* responds to the second of three assessment directives issued by the Deputy Secretary of Defense on June 1, 2000. The June 1, 2000 directive called for the establishment of a process review team [PRT] to assess DOD's plan to eliminate the backlog of overdue periodic reinvestigations by September 30, 2002. The PRT determined DOD would not meet the September 30, 2002 target date for elimination of the PR backlog. The PRT did not consider the submission of the overdue PR requests sufficient to eliminate the backlog. Rather, the PRT considers the backlog eliminated once the investigations have been completed and adjudicated and the workloads of DSS and the Central Adjudication Facilities [CAFs] return to a steady state.
- October 31, 2000—The report, *An Assessment of the Department of Defense Personnel Security Program,* responds to the first and third directive issued by the Deputy Secretary of Defense on June 1, 2000 to determine where DOD currently stands in reforming the PSI process, and recommend how to expedite the reform effort. The assessment team conducted a thorough review covering the major steps in the

PSI process including requesting the investigation, conducting the investigation, adjudicating the results of the investigation, and oversight and funding of the program.

- December 14, 2000—The Office of the Under Secretary of Defense (Comptroller) revised the Spend Plan to incorporate the adjustment of the backlog from 505,786 to 316,995 in accordance with the Process Review Team's survey results pursuant to the directive issued by the Deputy Secretary of Defense on September 11, 2000.
- February 8, 2001—Office of the Assistant Secretary of Defense (C3I) Security Directorate released the draft report, *Personnel Security Investigations: Mission Degradation,* which called for bold action to address current PSI backlogs. The purpose of the draft report is four fold: No. 1, to serve as a frame of reference for surfacing various options and reactions to organizations both within and outside the Department; No. 2, to be used to further refine the situation with those who are performing PSI work for DOD; No. 3, to serve as a think piece for DOD senior executives who will be reviewing the progress on balancing PSI funding and workload issues; and No. 4, to present options for consideration by the interagency.

On June 9, 1999, Deputy Secretary of Defense John J. Hamre issued a memorandum, "Personnel Security Clearance Investigations Backlog" directing the military departments, defense agencies, and contractors to eliminate the backlog by the end of fiscal year 2000.[81] This was the first of four target dates calling for the elimination of the PSI backlog.

In addition, the Deputy Secretary's memorandum of June 9, 1999 attempted to ease the pressure on DOD investigative capacity by shifting a part of the workload to the Office of Personnel Management. The memorandum also directed each service and DOD agency to provide the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence a quarterly plan for eliminating the backlog. The Deputy Secretary of Defense further directed the services and defense agencies to administratively terminate or downgrade all clearances not based on a current investigation or not in process for reinvestigation by September 30, 2000.[82]

On June 15, 1999, then Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Arthur L. Money issued a memorandum "Personnel Security Clearance Investigations backlog" implementing Deputy Defense Secretary's June 9, 1999 memorandum with respect to cost, process, and prioritization.[83] The memorandum directed all components to identify the resources necessary to fund the elimination of the backlog. The memorandum changed personnel security reinvestigation policy directing each service, agency, and contractor not to apply for security investigations for those within 1 year of separation from

[81] Memorandum: *Personnel Security Investigations Backlog,* June 9, 1999, from Deputy Secretary of Defense John J. Hamre to Secretaries of the Military Departments, et. al., (in subcommittee files).
[82] Ibid.
[83] See supra note 54.

DOD employment, or who will be assigned to duties for which a personnel security clearance is not required.[84] This policy change had serious national security implications by allowing a person to continue in a sensitive position without the required periodic investigation. The policy change was a violation of personnel security clearance standards adopted and approved by the Security Policy Board.

In that regard, even when the Deputy Secretary of Defense thought OASD (C3I) had a handle on the true size of the backlog, no provision was made for providing for additional funds to eliminate the backlog of PSI requests, nor was there any specific strategy available for processing the minimum number of additional PSI requests over and above those already programmed to be conducted.[85]

GAO also pointed out this directive had drawbacks, specifically the lack of funding. Carol Schuster stated, "We recommended to the Secretary of Defense to direct the Assistant Secretary of Defense (C3I) to identify and prioritize overdue investigations and fund and implement initiatives to conduct these investigations in a timely manner." [86]

On September 29, 1999, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Arthur L. Money issued a memorandum "Personnel Security Clearance Investigations" directing the submission of all initial investigations and reinvestigations of DOD civilian personnel to OPM effective October 1, 1999.[87] It stated DSS would continue to conduct investigations for military personnel, for civilian personnel stationed overseas, and for contractor personnel.[88]

By November 30, 1999, it became apparent the actions DOD had taken to date were not getting the results anticipated. As a result, Deputy Secretary of Defense called for the creation of an Overarching Integrated Process Team [OIPT] to find a solution for the backlog problem and to "pioneer a different path to solve the crisis of the continuing personnel security investigations backlog," and to submit a plan by January 20, 2000.[89]

The team reported their findings and recommendations in January 2000. The team determined the backlog totaled 505,786 and recommended additional personnel security investigation cases be transferred to OPM.[90]

As mentioned earlier, DOD's two attempts to determine the backlog size had methodological limitations, produced estimates that were 6 months old or older, and did not include thousands of overdue reinvestigations that had been submitted. The two estimates,

---

[84] Ibid.

[85] Memorandum: *Personnel Clearance Backlog and Security Initiatives,* June 22, 2000, from Under Secretary of Defense (Comptroller) William J. Lynn to Secretaries of the Military Departments, et. al., (in subcommittee files).

[86] Statement of Carol R. Schuster, Associate Director, U.S. General Accounting Office, NSVAIR Subcommittee hearing, Serial No. 106–152, p. 16.

[87] Memorandum: *Personnel Security Investigations,* Sept. 29, 1999, from Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Arthur L. Money to Secretaries of the Military Departments, et. al., (in subcommittee files).

[88] Ibid.

[89] Memorandum: *Personnel Security Investigations Backlog,* Mar. 31, 2000, from Deputy Secretary of Defense John J. Hamre to Secretaries of the Military Departments, et. al., (in subcommittee files).

[90] See supra note 43, p. 21–22.

one by the Overarching Integrated Process Team and the other by the MITRE Corp., were developed independently and used different estimating methods but coincidently arrived at similar estimates of about 505,000 overdue reinvestigations. These estimates differed from several previous backlog estimates that were cited by GAO in various DOD documents and statements.[91]

During the February 16, 2000 NSVAIR Subcommittee hearing, the DSS Director stated, "I am accepting their number. However, I do not have total confidence in it."[92] When asked to clarify this statement, the DSS Director said, "While the number (PSI backlog) could be lower, I think the number is higher. That is my professional judgment."[93] Carol Schuster, Associate Director of GAO concurred stating, "I cannot tell you what the size of the backlog is. I would really question whether they have an exact fix it on."[94]

This was finally confirmed by the Office of the Assistant Secretary of Defense (C3I) during the September 2000 NSVAIR Subcommittee hearing. "While there is some concern about the various methodologies used to arrive at the size of the backlog, it was acknowledged that a more accurate assessment would prove problematic. The difficulty in assessing the precise scope of the backlog is due to the limitations of the current DOD central clearance database, which contains records for approximately 2.5 million cleared DOD military, civilian and contractor personnel. This problem will be resolved when DOD fields the Joint Personnel Adjudication System in fiscal year 2001. JPAS will require continuous tracking (and input) of an individual's actual access requirement upon which the periodic reinvestigation is based."[95]

JPAS is designed to provide DOD with the ability to provide real-time data on the number of personnel currently authorized to have access to classified information, and will facilitate accurate forecasting of reinvestigation requirements. In addition, JPAS could further support reciprocity by including clearance data from non-DOD agencies.[96]

DOD stated, "JPAS will provide all DOD components, for the first time, a single, central, fully integrated system for managing their cleared personnel and providing accurate statistics on such things as projected periodic review requirements and whose PSI is pending or closed."[97] In addition, the DOD–IG reported, JPAS will provide DOD with a common information resource for granting and sharing personnel security eligibility determinations and recording personnel access to sensitive information.[98]

However, the projected ability to field JPAS in fiscal year 2001, once again, was overly optimistic. According to the DOD's Deputy

---

[91] See supra note 80, p. 6.
[92] See supra note 34, p. 111.
[93] Ibid.
[94] See supra note 11, p. 34.
[95] Statement of J. William Leonard, Deputy Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, NSVAIR Subcommittee hearing, Serial No. 106–267, p. 60.
[96] See supra note 37, p. 39.
[97] DOD response to *Questions for the Record Inquiry,* Mar. 27, 2001, House Government Reform Committee, NSVAIR Subcommittee, Defense Security Service hearing, Mar. 2, 2001, (in subcommittee files).
[98] Department of Defense, Office of Inspector General Audit Report, *Acquisition Management of the Joint Personnel Adjudication System,* Report No. D–2001–112, May 5, 2001, (in subcommittee files).

Inspector General, "Although the future Joint Personnel Adjudication System is the long term solution, it is agreed that the case control management system would be modified this year as an interim alternative. Due to subsequent slippage in baselining the system, the change may not be made until fiscal year 2002."[99]

Without knowing with any certainty the size of the PSI backlog but suspecting it could be higher, the DSS Director said at the February 16, 2000 NSVAIR Subcommittee hearing, "We believe that we can bring the backlog, as we now know it, we can eliminate the backlog by the end of calendar year 2001."[100]

The following month, DOD changed the PSI backlog elimination target date a third time. On March 31, 2000, Deputy Secretary of Defense John J. Hamre issued another memorandum,[101] "Personnel Security Clearance Investigations Backlog" directing the Military Departments, Defense agencies, and contractors shift all new Secret and Confidential level investigations to OPM through its contractor US Investigations Services [USIS] and changing the target date for elimination of the backlog to March 31, 2002.[102] DSS would retain responsibility for all top secret investigations and reinvestigations for military and contractor personnel. The objective was to reduce pressure on DSS for conducting hundreds of thousands of investigations while leveraging OPM's investigative capacity.[103]

On June 1, 2000, Deputy Secretary of Defense Rudy de Leon issued the memorandum, "Personnel Security Investigation Process Review" directing a comprehensive review of the personnel security process, to establish a "get well" date, and make additional recommendations to expedite the personnel security process effort. A Process Review Team was established to accomplish this effort.[104] Once again the Department was attempting to ascertain the size of the backlog and when it would be eliminated.

On June 22, 2000 Under Secretary of Defense (Comptroller) William J. Lynn issued the memorandum, "Personnel Clearance Backlog and Security Initiatives," generally referred to as the "spend plan."[105] The directive included monthly targets for all DOD components for submitting PSI requests to DSS and OPM, along with the associated funding to eliminate the backlog. The Comptroller estimated the Department would need an additional $201.6 million over 2 fiscal years to fund PSI cases taken over by OPM in addition to the funds already planned in the budget at that time.

The Department had finally recognized additional funding was needed to address the growing PSI backlog.

GAO had recommended as part of their review of the Personnel Security Investigation Program in October 1999 that DOD provide additional funding to address the PSI backlog. According to Carol Schuster, "One of the problems that has occurred over the last cou-

---

[99] Statement of Robert J. Lieberman, NSVAIR Subcommittee hearing, Serial No. 107–40, p. 17.
[100] See supra note 34, p. 114.
[101] See supra note 89.
[102] Ibid.
[103] Ibid.
[104] Memorandum: *Personnel Security Investigation Process Review,* June 1, 2000, from Deputy Secretary of Defense Rudy de Leon to Secretaries of the Military Departments, et. al., (in subcommittee files).
[105] See supra note 85.

ple of years is they have mandated (PSI) submissions, but the money has not been behind it. So the services have been cajoled to put in submissions, but the money has to be reprogrammed from other programs in order to cover it. That has been true for 1999, it has been true for 2000, and it is true for 2001. When the money is not there and the services choose not to reprogram the money for that purpose, then the submissions are not made."[106] The Comptroller also moved the backlog elimination target date to September 30, 2002.[107]

The "spend plan" mandated that each DOD component submit a designated quota of backlogged cases each quarter of fiscal year 2001 and fiscal year 2002. If implemented as planned, all backlogged cases as of September 2000, were to be submitted by the end of fiscal year 2002. These cases were to be in addition to those cases coming due for reinvestigation and new cases. Together, these new submissions represented a very large influx of cases given that there was already a large backlog of unprocessed cases at DSS. GAO had estimated that the number of PSI cases involved was 2.2 million, raising additional concerns.

Several other attempts were made to increase capacity to process PSI cases. These included entering into contracts with private sector investigative firms and bringing a number of reservists onto active duty to assist DSS.[108] General Charles J. Cunningham Jr., USAF (Ret), Director, Defense Security Service informed the subcommittee, "Our plan to use private sector contractors to augment our investigative workforce has continued to materialize and is proving to be a successful endeavor. In addition, to contractor augmentation, we are also using military reservists to augment our investigative workforce. Currently, approximately 45 reservists who have prior investigative and interviewing experience are integrated into our agent workforce."[109]

Although these were positive steps, they were not seen as enough to handle the increase in PSI cases expected as a result of the implementation of the spend plan. According to GAO, "it's really hard to tell exactly what kind of an effect this large influx of cases is going to have and whether the use of private contractors and reservists and the like are going to make a dent in that."[110]

Carol Schuster stated, "we've already gone over how flimsy the 500,000 is so we don't really know whether that's a good estimate or not. We do know how many cases are called carryover cases-those already submitted to DSS. Over the next 2 years, they've got 435,000 of those cases. Then you've got the backlogged cases and then you've got new cases coming in. So all told, we're talking about an enormous workload here of 2.2 million cases coming into the investigative community. As I understand it, the spend plan for this 2-year period is just to get the cases submitted, and then it is up to the investigative community to somehow deal with that. We haven't really seen the influx yet. A lot of the cases that are

[106] See supra note 11, p. 47.
[107] See supra note 85.
[108] See supra note 36, p. 78.
[109] Ibid.
[110] See supra note 11, p. 46.

going to OPM really start at the beginning of the fiscal year in October (2000)."[111]

Other efforts to reduce the backlog and identify potential high-risk cases included the development of a predictive model or algorithm to track those cases. Carol Schuster stated, "They are taking several actions. One in particular, I think, is very promising. They are working on an algorithm that will try to identify those cases that are most likely to result in a denial of a clearance, based on their past experience. That will allow them, if they can get this to work, to identify those cases that are most risky to the government and be able to process those in a priority manner." [112]

During the subcommittee's DSS oversight hearing in February 2000, DSS Director General Charles J. Cunningham submitted written testimony which stated, "DSS has established several initiatives to more effectively manage this significant increase in clearance demand while at the same time reducing the inherent risks associated with outdated investigations in individuals already accessing classified information, thus reducing the vulnerability of insider threat. One of those initiatives is the development of a predictive model to identify those cases that pose a higher risk based on responses to certain questions on the personnel security questionnaire. The algorithm will be applied at the front end of our investigative process to ensure that the potential high-risk investigations receive priority processing." [113]

The MITRE Corp. was retained by DSS to develop the algorithm. The MITRE Corp. produced "a statistically based prioritization procedure whereby a high percentage of the 'latent revocations' among the backlog could be identified and given immediate attention, based solely on the information provided in a standard Electronic Personnel Security Questionnaire [EPSQ]. Such a method would allow the DSS to allocate limited investigative resources so as to remove a high percentage of the risky backlog cases in the shortest amount of time." [114]

Responding to the question of what kind of risk assessment had been developed to determine the danger the backlog poses to national security, the DSS Director stated, "GAO mentioned the algorithm that we have been working on and we have now completed. Our plan is to go into the total population of the backlog, apply the algorithm, identify which records come up as high risk from the algorithm, which we believe and have had scientific support will predict 89 percent, based on a 6.5 percent sample size, that we use it against the backlog while we are bringing the backlog down. So that we both work the backlog down and, in the process, go after those that are identifiable as highest risk in the backlog." [115]

At that time, General Cunningham indicated DSS expected to implement an algorithm and have a prioritization process for back-

---

[111] Ibid.
[112] See supra note 75, p. 22.
[113] Statement of Lt. General Charles J. Cunningham Jr., USAF (Ret), Director, Defense Security Service, Serial No. 106–152, p. 54.
[114] See supra note 61, p. iii.
[115] See supra note 34, p. 114.

log cases by July 2000. The algorithm for identification of high-risk cases was implemented in November 2000.[116]

The prioritization of backlog cases proved even more difficult to implement. As a result, the lack of any effective priority tracking procedures has subjected DSS to criticism from both the DOD–IG and the services. In April 2000, an Office of the Inspector General [OIG] audit report recommended that the Office of the Assistant Secretary of Defense (C3I) develop criteria to determine the highest priority mission-critical and high-risk positions based on their impact on mission-critical programs.[117]

According the Acting Inspector General, "I think the only way to really handle the problem is to allow the various DOD components the opportunity to prioritize what they feel is truly important in their work, and to, therefore, fit those concerns into the plan. So I think it should be on a broad basis and not just for a few of the high-risk programs. When you're seeking consensus and agreement on how to prioritize, it's going to take a while longer than it would take to simply direct it from the top. It is my understanding that process is continuing, that the Department hopes to have some sort of process in place in the next few months." [118]

The Acting Inspector General went on to say, "The clearance requests for important programs and higher risk programs often languished while investigators often worked routine cases. The Office of the Assistant Secretary of Defense (C3I) initially disagreed with the feasibility of developing a prioritization method but has subsequently changed its position and has been working with the services and DSS to comply with the recommendation. I'm still frankly disappointed, however, with the slow progress, and am concerned that it appears so difficult to implement what is to us a basic workload management tool. We believe this delay was unnecessary and could have been avoided through firm decisionmaking by leadership." [119]

Due to DOD component resistance and ongoing CCMS problems, DSS did not expect to implement a risk prioritization process until January 2001. Regarding the implementation of a prioritization process, the Deputy Assistant Secretary of Defense (Security and Information Operations) stated, "the recent problems with CCMS and the resulting increase in DSS case completion times, prioritization has become problem as case completion times have soared to a year or more in some cases. The OSAD (C3I) has taken the lead in developing with the DOD component customers a draft prioritization plan." [120] A prioritization process for backlog cases was not implemented in January 2001.[121]

In March 2001 the subcommittee learned, from the Assistant Secretary of Defense (C3I) Arthur L. Money, "CCMS, which is part of all of this, is getting more stable and better, but it needs a prioritization application program added to it so we can prioritize

---

[116] See supra note 97.
[117] Department of Defense, Office of Inspector General Audit Report, *Security Clearance Investigative Priorities,* Report No. D–2000–111, Apr. 5, 2000, Executive Summary, p. 14, (in subcommittee files).
[118] See supra note 70, p. 44.
[119] Ibid., p. 21.
[120] See supra note 95, p. 66.
[121] Ibid., p. 67.

things, and that is what that report (*Personnel Security Investigations: Mission Degradation*) pointed out. That internal report pointed out that we do not have prioritization within DSS, which is being fixed and will be in place in April 2001." [122]

On August 22, 2000, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Arthur L. Money issued a memorandum "Personnel Security Clearance Investigations" implementing the Deputy Secretary's direction to distribute the personnel security clearance workload between DSS and OPM.[123]

The Assistant Secretary also directed military departments, defense agencies, and contractors, per the Comptroller's "Spend Plan," to appoint a senior official to oversee the execution of their workload plan. Under DOD Directive No. 5200.2 issued April 9, 1999,[124] DOD components had previously been directed to designate a senior official to implement and administer the DOD Personnel Security Program. The senior component official would be responsible for monitoring and reporting the status of availability of sufficient funds, ensuring the PSI backlog workload distribution is maintained, and ensuring the timely adjudication of completed cases.

On September 11, 2000, Deputy Secretary of Defense Rudy de Leon issued a memorandum, "Personnel Security Investigation Review" directing military departments, defense agencies, and contractors to review their requirements for personnel security reinvestigations.[125] The Process Review Team that the Deputy Secretary created on June 1, 2000 determined that the backlog baseline had changed due to lapse of time and the efforts of the components in submitting personnel security reinvestigation requests. An update of the backlog was considered essential for planning and funding decisions. The results indicated that the backlog had dropped by 187,677 cases from 505,786 as reported in January 2000 to 318,109 in just 6 months.[126]

On October 11, 2000, the Deputy Secretary's Process Review Team formally reported the results of their review analyzing when DOD should expect the PSI process to "get well" as tasked by the Deputy Secretary's memorandum of June 1, 2000.[127] The Process Review Team report revealed a dispute over what PSI cases were to be considered as part of the backlog. The OASD (C3I) considered the backlog eliminated when all of the overdue PRs have been completed for investigation. "Although, this goal represents an important milestone, a process review team reported, the elimination of the backlog means completion of investigations associated with

---

[122] Testimony of Arthur L. Money, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, NSVAIR Subcommittee hearing, Serial No. 107–40, p. 55.

[123] Memorandum: *Personnel Security Clearance Investigations,* Aug. 22, 2000, from Assistant Secretary of Defense for Command, Control, Communications, and Intelligence Arthur L. Money to Secretaries of the Military Departments, et. al., (in subcommittee files).

[124] Department of Defense Directive, No. 5200.2, Apr. 9, 1999, DOD Personnel Security Program, (in subcommittee files).

[125] Memorandum: *Personnel Security Investigation Review,* Sept. 11, 2000, from Deputy Secretary of Defense Rudy de Leon to Secretaries of the Military Departments, et. al., (in subcommittee files).

[126] An Assessment of DOD's Plan to Eliminate the Periodic Reinvestigation Backlog, A Report to the Deputy Secretary of Defense, Personnel Security Investigations Process Review Team, Oct. 11, 2000, p. 4, (in subcommittee files).

[127] Ibid.

those PRs, the adjudication of the investigations, and a return of the pending workload to steady state."[128] The Process Review Team considers the backlog eliminated once the investigations have been completed *and* adjudicated and the workloads of DSS and the Central Adjudication Facilities [CAFs] return to steady state. "Assuming that DSS completes the last backlog investigation by mid to late FY2003, the last backlog cases would be adjudicated not later than the end of FY2003. At that time, the backlog will be eliminated and investigative workload will return to a steady state."[129] This marked the fifth time in a 1½ year period that the target date for elimination of the backlog moved farther down range.

Commenting on DOD's ability to carry out this plan and achieve the new benchmark date for the elimination of the backlog, Deputy Inspector General Robert J. Lieberman said, "As far as the prospects for execution of the current plan are concerned, I don't think that we can be fully confident that we understand how many new investigations are going to be required until the system that Mr. Money referred to, the new system that is just being fielded now, is actually in place and starts generating experience data that we can all rely on. I think in another year or so we will be looking at the numbers again and perhaps the plan does not have to be stretched out. It may be evident that we will achieve this steady-state sometime earlier, but my guess is that we will not be seeing this steady-state for a few months after the end of the project plan."[130]

On October 31, 2000, the Deputy Secretary's Process Review Team responded to the remaining tasks as directed by the Deputy Secretary's memorandum of June 1, 2000. This report responds to the first and third tasks, to determine where DOD currently stands in reforming the PSI process with recommendations of how to expedite this reform effort.[131]

On December 14, 2000, the Office of the Under Secretary of Defense (Comptroller) issued a revised spend plan to incorporate the adjustment of the backlog from 505,786 to 318,109 in accordance with the process review Process Review Team's survey results. The report included performance expectations for completing personnel security investigation cases and a $44.1 million reduction in funding for fiscal year 2001 and fiscal year 2002.[132]

On February 8, 2001, the Director of Security, OASD (C3I) released a draft report on the status and possible options regarding the conduct of personnel security investigations by DSS.[133]

The draft report indicated, "the time to complete the types of investigations upon which clearances are based was getting longer, not shorter."[134] As the time to complete investigations has grown, the number of investigations pending also grew. "If this trend remains static, there is no probability that the backlog of periodic re-

[128] Ibid., p. 5.
[129] Ibid., p. 4.
[130] Testimony of Deputy Inspector General, Robert J. Lieberman, NSVAIR Subcommittee hearing, Serial No. 107–40, p. 37.
[131] See supra note 37.
[132] Department of Defense, Office of the Under Secretary of Defense (Comptroller), *Plan for Eliminating the Personnel Security Investigation Backlog,* Dec. 14, 2000, (in subcommittee files).
[133] See supra note 43.
[134] Ibid., p. 4.

investigations will be reduced by the end of FY 2002, as currently directed." [135] However, according to Assistant Secretary of Defense Arthur L. Money, "the draft report was not reviewed; and it is not entirely accurate. You will see it has 'draft' on it and so forth, so it was a failing within my office of not having the report vetted and made more accurate." [136]

Commenting on the February 8, 2001 draft report, the Deputy Inspector General stated, "It is likely that much of the data being used to track progress against the plan is flawed, but the errors are probably not egregious enough to distort the overall trends, which are very disappointing." [137]

The draft reports states quite clearly, "When observed as a whole, the current process as defined by the various directions and plans contained in the policy memoranda that have been issued by senior DOD management since June 1999, is not meeting the Department's need to provide timely investigations and clearances." [138] When queried further why the draft report shouldn't be given more creditability, the Deputy Assistant Secretary J. William Leonard said the draft report did not include the PSI workload completed by OPM. Secretary Leonard said if the draft report had included the OPM workload, DDS turnaround time for completed PSIs would have been lower. "When we were here last September (2000), we reported to the committee that a good part of our plan encompassed off-loading work from DSS to OPM. So therefore, any assessment of that plan would have to take into account what OPM is doing." [139]

OPM had the capacity to handle personnel security investigations, and after 1 year demonstrated the ability to complete those investigations transferred from DSS in an accurate and timely manner.[140] OASD (C3I) senior management wanted the subcommittee to accept the argument that the draft report was flawed because the authors did not include OPM's statistics in the calculation of the number of cases processed and how long it was taking to process those cases. As Mr. Leonard went on to say, "And so, for example, for the first quarter OPM did, I believe close to 28,000 investigations for the Department of Defense, and if they were factored into case completion times, for example, what it would have shown is that Department-wide case completion times actually decreased." [141] DSS was taking credit for OPM's ability to complete personnel security investigations in a timely manner and wanted to include those figures in a report that would have shown improved progress.

Also, it should be noted the composition of the investigations handled by each is not the same. OPM handles many cases that can be processed by simple computerized checks, whereas almost all of DSS workload involves the most labor-intensive and time-consuming background investigation work related to top-secret clear-

---

[135] Ibid., p. 10.
[136] See supra note 122, p. 54.
[137] See supra note 99, p. 14.
[138] See supra note 43, p. 4.
[139] Testimony of J. William Leonard, Deputy Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, NSVAIR Subcommittee hearing, Serial No. 107–40, p. 61.
[140] See supra note 126, p. 15–16.
[141] See supra note 139, p. 61.

ances. Therefore, the time necessary to complete a case varies widely between DSS and OPM. The handling of PSIs by OPM was not intended to be a permanent fix and as such should not be included in any measurement of DSS's workload capacity.

When pressed further regarding the accuracy of the draft report relative to the Department's need to provide timely personnel security investigations and clearances, Deputy Assistant Secretary J. William Leonard stated, "Don't get me wrong. I am not saying that we are where we want to be. We recognize that we are not on a glide path, so from that point of view, the fundamental thing you get out of that report is accurate. And we are very mindful of that and we are focused on that." [142]

The January 2002 Department of Defense, Office of the Inspector General semi-annual report to Congress highlighted "The inability of the Defense Security Service Program to ensure timely investigations also remains a serious concern. The Defense Security Service has increased its productivity and the Office of Personnel and Management has provided good support through its contractors to work off the backlog of several hundred thousand overdue clearance investigations and achieve reasonable turnaround times for new investigations requests. The program remains hampered, however, by uncertain projections of the future investigative workload. There is widespread skepticism among DOD components about the ability of DSS to efficiently handle more workload, yet DSS views the outsourcing of much of the investigative workload to OPM as a temporary measure. The long delayed transition of DSS to a pay-for-service organization remains a key DOD management objective, but DSS still lacks a cost accounting system." [143]

2. There was a lack of management oversight of the Defense Security Service [DSS] by the Department of Defense that contributed to a backlog of personnel security investigations.

The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [C3I] is the Department of Defense's senior agency official responsible or the personnel security program. Responsibilities of the Assistant Secretary (C3I) include oversight of the Defense Security Service, and direction, administration and oversight of the DOD personnel security program.[144]

In addition, the DOD Personnel Security Committee [DODPSC] and Executive Steering Group [ESG] were established in 1999 to provide input and support to DOD's personnel security program management.[145]

In 1999, the General Accounting Office reported the Defense Security Service operated for at least 4 years with little or no oversight from the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence [C3I] which is responsible for assessing the completeness of DSS investigative work.[146]

---

[142] Ibid.
[143] Inspector General, Department of Defense, Semi-Annual Report to Congress, Apr. 1–Sept. 30, 2001. p. 3.
[144] See supra note 37, p. 44.
[145] Ibid.
[146] See supra note 27, p. 29.

Substantiating this in his prepared statement for the March 2, 2001 NSVAIR Subcommittee hearing, Deputy Inspector General Robert J. Lieberman stated, "senior DOD leaders paid very little attention to the Defense Security Service before the crisis broke." [147]

A report, issued October 31, 2001, to the Deputy Secretary of Defense assessing the personnel security program observed oversight of the personnel security program by the Office of the Assistant Secretary of Defense (C3I) had not been effective.[148] DOD officials told GAO that once DSS became a reinvention laboratory, it was allowed to operate, for the most part, independently.[149]

As an example, from August 1996 through February 1999, DSS relaxed its investigative requirements through a series of policy letters.[150] Several of these letters gave investigators greater discretion in how they would meet the Federal standards or pursue investigative issues that might be significant. These policy changes caused much confusion among agency staff.[151]

In 1996 and again in 1998, the Security Policy Board advised DSS not to adopt policies that ran counter to the Federal investigative standards.[152] The Director of the Security Policy Board staff stated, "Apparently, rather than fight for adequate funding, DSS has chosen an assault on personnel security clearance standards." [153]

The Board noted that DOD was a full partner in developing the new standards and that the planned actions by DSS would undermine the objectives of achieving reciprocity and PSI standardization among Federal Government agencies, cause a serious deterioration in the quality of investigative work, and increased security risk. The Policy Security Board stated that if DSS wanted to change the standards the agency should bring such requests to the Board, which was specifically established for that purpose. According to GAO, in spite of this advice, DSS management adopted the relaxed investigative guidance.[154]

When questioned how lack of oversight and mismanagement of the agency contributed to PSI weaknesses found in GAO's review of the Personnel Security Investigation Program, Carol R. Schuster, Associate Director, stated, "We found weaknesses in several areas. The first area was relaxing the standards below Federal standards, and also allowing perhaps too much latitude with their investigators as to how far and how deeply they went into the investigative areas. The second area was doing away with some of the quality control mechanisms they had on those investigations. They did away with the Quality Assurance Branch, and supervisory review, for instance. In the training area, they just really were not giving very much training to the investigators. Because there were new investigative standards, there was a need for such training. They also did away with the Security Institute, which was

---

[147] See supra note 99, p. 9.
[148] See supra note 37, p. 9.
[149] See supra note 27, p. 29–30.
[150] Ibid., p. 20.
[151] Ibid. p. 21.
[152] See supra note 41.
[153] Ibid.
[154] See supra note 86, p. 13–14.

training not only to DSS investigators, but investigators throughout the Government." [155]

The lack of oversight also affected the acquisition of the Case Control Management System. The Office of the Assistant Secretary of Defense (C3I) has the responsibly for monitoring major IT acquisitions.[156] Robert J. Lieberman, Deputy Inspector General stated, "we have spent about $100 million so far on CCMS." [157]

During the September 20, 2000 hearing, the subcommittee learned CCMS would be designated a major acquisition project 4 years after the project began. In his prepared statement Donald Mancuso, Acting Inspector General wrote, "We understand that the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) intends to designate CCMS as a major acquisition project, meaning there will be oversight by an Integrated Process Team and the Chief Information Officer [CIO] at the Office of the Secretary of the Secretary of Defense level. This is a prudent step, but does not in itself guarantee close oversight." [158]

When acquiring major IT systems, the Clinger-Cohen Act [159] requires the Chief Information Officer [CIO] to monitor and evaluate the performance of information technology programs and advise the heads of agencies whether to continue, modify, or terminate a program.[160] Carol R. Schuster, Associate Director, stated, "to my mind (CCMS) is the biggest challenge that they face. That automated system was just not planned properly. It was not implemented properly. The people who were trying to procure that system and manage it really were not totally qualified to do that. They did not have the background in a major acquisition program. They did not have the information technology expertise to really do that." [161]

Arthur J. Money, Assistant Secretary of Defense (C3I) conceded CCMS oversight failures stating, "A program that had started in 1995, called case control management system, was installed. Now, here was a major failure. It was installed without testing, and the legacy system was turned-off never to be turned back on, or never could be turned back on." [162]

And, acknowledging the lack of acquisition and deployment oversight of CCMS by the Office of the Assistant Secretary of Defense (C3I), the Deputy Assistant Secretary of Defense J. William Leonard stated, "I am sitting here before you with the full knowledge that a significant part of the solution is to address shortcomings in past oversight from my organization, especially with respect to things such as overseeing the acquisition of a major automation system such as CCMS. I recognize that and am very much committed personally and organizationally to ensure that we address these issues in the months to come." [163]

---

[155] See supra note 75, p. 19.
[156] See supra note 28, p. 3.
[157] Testimony of Deputy Inspector General, Robert J. Lieberman, NSVAIR Subcommittee hearing, Serial No. 106–267, p. 36.
[158] Statement of Donald Mancuso, Acting Inspector General, DOD, Office of the Inspector General, NSVAIR Subcommittee hearing, Serial No. 106–267, p. 34–35.
[159] 41 U.S.C. Sec. 251 (The Clinger-Cohen Act of 1996).
[160] See supra note 98, p. 7.
[161] See supra note 75, p. 22.
[162] See supra note 122, p. 36.
[163] See supra note 95, p. 54.

However, in that regard, there was more involved in the failure of CCMS than just software and design problems. In December 2000 the DOD Inspector General indicated in an audit of the case control management system that "despite the key roll of CCMS in DSS operations that support virtually all DOD critical missions, minimal acquisition oversight and guidance was provided or offered by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence." [164]

Others have also noted the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (OASD–C3I) had difficulty providing adequate management oversight. The Report of the Commission to Assess U.S. National Security Space Management and Organization noted, "The current ASD (C3I) organization suffers from three difficulties: the span of control is so broad that only the most pressing issues are attended to and (space) matters are left, on a day-to-day basis, in the hands of middle-level officials without sufficient influence within the Department and the interagency arena." [165]

Insufficient influence within the Department and interagency arena was again evident in an OASD (C3I) August 22, 2000 directive [166] concerning compliance with a newly established workload plan for the elimination of the PSI backlog. The Assistant Secretary of Defense (C3I) merely "*encouraged* (emphasis added) the Military Departments and Defense agencies to have their Inspectors Generals include compliance as a matter of interest during inspections for FY2001 and FY 2002 to preclude the recurrence of the PSI backlog." [167] As the PSI backlog grew to crises proportions, the Assistant Secretary of Defense (C3I) should have been made clear the PSI backlog should be treated more than just as a matter of interest.

3. Acquisition of the Case Control Management System [CCMS] and the Joint Personnel Adjudication System [JPAS] did not comply with the requirements of the Clinger-Cohen Act and may not provide effective caseload management.

The Office of the Assistant Secretary of Defense (C3I) is responsible for overseeing the design and implementation of large information technology systems are on schedule, within acceptable cost parameters, and have full user satisfaction. The Subcommittee found the Office of the Assistant Secretary of Defense (C3I) has a poor record for controlling the proliferation of incompatible IT systems, acquiring new systems that meet user needs within reasonable timeframes, controlling acquisition and upgrade costs, and ensuring the quality of data.

---

[164] See supra note 28.
[165] Public Law 106–65, Report of the Commission to Access United States National Security Space Management and Organization, *Executive Summary,* Jan. 11, 2001, p. 21, (in subcommittee files).
[166] See supra note 123.
[167] Ibid.

As a result, the Office of the Assistant Secretary of Defense (C3I) allowed the acquisition and development of CCMS [168] and JPAS [169] without first determining whether the systems were the most cost-efficient and cost-effective solution for opening, tracking, closing, and adjudicating personnel security investigation cases.

The lack of oversight resulted in the deployment of a major IT system, the case control management system, that has put national security at risk and will require millions of additional dollars to fix or replace. The Defense Security Service's deployment of CCMS resulted in decreased productivity contributing to the periodic reinvestigation backlog. CCMS has become a costly attempt to maintain a failing status quo despite recommendations to scrap the system.[170] DSS will spend more to fix the CCMS than it cost to acquire it.[171]

CCMS was designed to guide and control the Defense Security Service Enterprise System for opening, tracking, and closing personnel security investigation cases. The Enterprise System is a combination of 24 distinct primary information systems, subsystems, applications, and interfaces that share common data and connectivity.[172]

Commenting on the acquisition of CCMS, the Acting DOD Inspector General Donald Mancuso stated, "The need for a modern DSS system with the capabilities intended for CCMS is undeniable; however, as has often been the case over the last decade with DOD information technology investments, execution of this system acquisition project was flawed. In retrospect, DSS and its contractors badly underestimated the technical risk and failed to test adequately to manage those risks." [173]

DSS believed establishing a paperless Enterprise System of automated applications would avoid as much as $80 million in operating costs over a 6 year period and $900 million over a 3 year period in reduced time for personnel security investigations.[174] Without knowing the extent to which CCMS is meeting cost and benefit expectations, DOD was not in a position to make informed decisions on whether to deploy the system.

Federal information technology investment management guidelines require Federal agencies to economically justify IT projects before investing in them, and to justify them in an incremental manner to spread the risk of doing many things over many years on large projects.

In December 2000, the DOD Office of the Inspector General issued an Audit Report citing DSS for not effectively managing the high risk involved in the acquisition and integration of CCMS and its Enterprise System by following the requirements of the Clinger-Cohen Act of 1996,[175] OMB Circulars and DOD guidance for acquisition of information technology systems. The Clinger-Cohen Act re-

---

[168] The case control mangement system was deployed in October 1998.
[169] The Air Force is testing and deploying JPAS. Current legacy adjudication systems will operate in parallel with the deployed JPAS. Initial operational capability is planned for October 2001.
[170] See supra note 36, Sec. 7, p. 67–68.
[171] Ibid., p. 1–7.
[172] See supra note 28, p. i.
[173] See supra note 158, p. 33.
[174] See supra note 28, p. i.
[175] Ibid., p. 3.

quires agencies to design and implement a process for assessing and managing the risks of information technology acquisitions to include analyzing, tracking, evaluating, and reporting on risks and results of all major information technology capital investments.[176] In addition, DOD regulations require every system acquisition program to establish cost, schedule, and performance objectives and thresholds before a major IT system is deployed.[177]

In February 2000, Carol Schuster, Associate Director of GAO's National Security International Affairs Division stated, "DSS did not properly plan for the implementation of a new system (CCMS) designed to automate its personnel security investigation case processing. As a result, DSS has not been able to process its investigations, the volume of investigations sent to field offices and adjudication facilities has decreased sharply, and according to DSS officials, DOD may have to add $100 million to $300 million more to the $100 million already spent on its automation efforts to have a workable system. The automation efforts have exacerbated DSS's efforts to cope with the large backlog of overdue investigations." [178]

Carol Schuster went on to say, "the basic underlying factors are that it really was not planned very well as an acquisition program. The people were not very well qualified in either IT or acquisition management." [179] DOD's Acting Inspector General Donald Mancuso concurred stating, "The failure of CCMS, the DSS case control management system, was also a major setback." [180] The DOD–IG reported, "Prior to September 2000, neither the CCMS nor the rest of the Enterprise System was designed as a major automated information system or a special interest initiative. Funds contractually obligated for the Enterprise System's development and modernization amounted to $76 million from FY 1995 through FY 1999. Total planned development and operation costs for FY 2000 through FY 2007 are estimated to be $312 million." [181]

When questioned what was the biggest problem the agency faced, the Director of DSS stated, "It is the case control management system because it becomes the pacing item for everything else that happens in the agency in investigations." [182] And, Assistant Secretary Money stated, "What happened in October 1998 was, essentially everything came to a grinding halt in that no cases were coming out due to software failure, system failures, and I will assert due to poor design on what CCMS ought to be." [183]

The Office of the Assistant Secretary of Defense (C3I) and the Defense Security Service are attempting to resolve CCMS technical and program problems by initiating a series of actions designed to improve and enhance system performance. In August 1999, recognizing the agency did not have the capability or in-house expertise to manage and support the case control management system, DSS transferred management of the system to the Air Force.

---

[176] Ibid., p. 15.
[177] DOD Regulation 5000.2–R, Mandatory Procedures for Major Defense Acquisition Programs and Major Automated Information Systems Acquisition Programs, Mar. 15, 1996 (revised June 2001), (in subcommittee files).
[178] See supra note 86, p. 15.
[179] See supra note 75, p. 32.
[180] See supra note 70, p. 20.
[181] See supra note 28, p. 2.
[182] See supra note 34, p. 117.
[183] See supra note 122, p. 36.

In addition, DSS is implementing a strategy to repair CCMS technical and program problems to improve the system's ability to open, track and close personnel security investigation cases. The aim is to expand the utility, efficiency, and effectiveness of CCMS to meet projected workload increases resulting from implementation of the spend plan.

The strategy will involve a three-phase process and timetable: Phase one would stabilize the existing system; phase two would improve the current system; and the third phase would implement enhancements to CCMS. Those enhancements, called "target architecture," would be developed and implemented over 5 years starting in fiscal year 2002. DSS has requested an additional $93 million to develop and implement phase three.[184] According to the Director of DSS, "This target architecture provides a framework for future development and implementation of the entire Defense Security Service Enterprise System, including the case control management system."[185] DSS believes the three-phase approach will not only allow for stabilization of the system and improvements to CCMS, but will preserve the initial investment in the system.

The August 22, 2000 memorandum issued by the Assistant Secretary of Defense (C3I) included detailed instructions to the DOD components transferring a portion of the personnel security clearance workload to OPM to fulfill the comptroller's spend plan directive. In part, this action was taken in an attempt to relieve the pressure on CCMS thereby allowing the system to more rapidly process incoming background investigations.[186] However, according to TRW, the case control management system's serious weaknesses will be far more difficult to fix than DSS anticipates.[187]

In December 2000, the DOD Inspector General recommended the Assistant Secretary of Defense (C3I) analyze whether the investment for the Case Control Management System provides the best business solution when compared to alternative solutions for opening, tracking, and closing personnel investigation cases.[188]

In January 2001, responding to the DOD IG's recommendation, the Assistant Secretary for Defense (C3I) wrote, "DSS and C3I concur with the finding and recommendation as stated in the DOD IG report. We will conduct an analysis of alternatives to support the direction we plan to achieve for the future architecture and will include the economic analysis and calculation of the return on investment. In addition, performance measures and information assurance requirements will also be addressed."[189]

As criticism of OASD (C3I) and DSS intensified over the handling of the case control management system, and as questions were raised regarding the justification for spending more to fix the system than it originally cost to purchase, DSS brought in consult-

---

[184] Letter from Lt. Gen Charles J. Cunningham, Jr., USAF (Ret), Director, Defense Security Service to Congressman Christopher Shays, chairman, NSVAIR Subcommittee, July 26, 2000, (in subcommittee files).

[185] See supra note 35, p. 77.

[186] See supra note 95, p. 62.

[187] See supra note 36, p. 1–5.

[188] See supra note 28, p. ii, (in subcommittee files).

[189] Memorandum: *Audit Report on Program Management of the Defense Security Service Case Control Management System (No. D–2001–019), Jan. 23, 2001, from Arthur L. Money, Assistant Secretary of Defense (C3I) to the DOD IG Office of Assistant Inspector General for Audit, Director, Acquisition Management (in subcommittee files).*

ants to evaluate the system. Carol Schuster stated, "Regarding past evaluations, there was a DOD red team that came in, and evaluated what they should do with that system, and what went wrong with the system, and what they would recommend. A TRW contractor evaluation also looked at it from a technical standpoint." [190]

The assessments found deficiencies in acquisition strategy, program management, system integration, and operations and maintenance. TRW estimated that an additional $168 million would be needed over the next 7 years to address these deficiencies for a system that was projected to cost $100 million when fully operational. Ultimately, TRW believed CCMS could not be reengineered cost-effectively and recommended scrapping the system altogether. "It is our engineering judgment that CCMS is not viable long-term and that it should be replaced. Such a replacement should be developed under the auspices of a strong, acquisition-experienced program management office." [191]

Carol Schuster stated, "Both of those groups pointed out numerous problems with the way the thing was put together, the lack of documentation, the lack of checks and controls, just what you would expect of an automated system, to the point that the TRW investigation did not feel like it was salvageable." [192]

Despite the criticism, DSS persisted in plans to spend more to fix CCMS, and contracted with TRW for a follow-up, independent evaluation. In response to an inquiry from the chairman of the NSVAIR Subcommittee regarding the justification of continuing investment in CCMS, DOD responded, "TRW reported in October 2000 that they now believe it is possible to retain and reuse substantial parts of the system. The system has sufficient stability to support operations for the foreseeable future. As improvements are made, alternatives are reviewed for impact and application for the various subsystems. No commitment to a future architecture for CCMS will be made without first conducting a thorough analysis of alternatives." [193]

During the October 2000 NSVAIR Subcommittee hearing, addressing the CCMS issue, the Director of DSS stated, "there were dramatic improvements resulting from the software enhancements and corrections that have been implemented within the last six months."[194]

In May 2001, responding to questions [195] for the record from the NSVAIR Subcommittee, the Office of the Assistant Secretary of Defense (C3I) reported, "The case Control Management System is not contributing to any increase in the pending backlog. CCMS has been stabilized and recent improvements allow the Defense Security Service to take advantage of the original functional design to minimize human intervention and repetitive tasks. Efforts were refocused on stabilizing and improving the system to ensure a productive system. Actions were taken as necessary to meet directed policy scope changes, to baseline the current system, and to sta-

[190] See supra note 75, p. 23.
[191] See supra note 36, p. 1–5.
[192] See supra note 75, p. 23.
[193] See supra note 97.
[194] See supra note 35, p. 75.
[195] See supra note 97, p. 8.

bilize key processing functions. While we have taken advantage of the original CCMS functions as intended, the changing PSI and technology requirements dictate an assessment of needs for the current baseline as well as future requirements. Future target architecture and business process reengineering requirements are in the concept stage with a formal Analysis of Alternatives scheduled for early fiscal year 2002." [196]

Also in May 2001, the DOD–IG issued an audit report [197] regarding the acquisition management of the Joint Personnel Adjudication System. JPAS will provide DOD with a common information resource for granting and sharing personnel security eligibility determinations and recording personnel access to sensitive and nonsensitive compartmented information. Its common database, linked by the Joint Adjudication Management System [JAMS] and the Joint Clearance and Access Verification Management System [JCAVS] applications, will standardize security clearance adjudications in compliance with DOD Regulation 5200.2–R,[198] and will provide security managers with eligibility verifications for personnel desiring access to sensitive and classified facilities, weapon systems, and information. JPAS will also provide reports for programming and managing workloads at the Central Adjudication Facilities [CAFs] and locations requiring cleared personnel.[199] JPAS is expected to minimize work delays for newly hired and visiting personnel with adjudicated clearances.[200]

As with CCMS, OASD did not manage the JPAS as an information technology investment when the acquisition strategy changed from a network of distributed database systems to a centralized database system.[201] The DOD Chief Information Officer [CIO] did not demonstrate oversight involvement in the acquisition of the JPAS. JPAS supports the eligibility adjudication and verification business processes for granting security clearances to military, civilian, and contractor personnel. Accordingly, any processing delay caused by JPAS could also delay DOD and contractor personnel from performing assigned functions. As a result, JPAS requires CIO oversight because of its significance in supporting DOD missions." [202]

4. There are no common standards for investigating and adjudicating a personnel security clearance in a timely manner.

The subcommittee found there were no clear timeliness standards for completing a personnel security clearance. As an example, the length of time for completing a top-secret clearance by the Defense Security Service in 2000 ranged from 298 days to 376 days.[203] Completion times by OPM were lower.

The DSS Director General Cunningham indicated as a result of reforms instituted, the agency would be able to do a case in 180

---

[196] Ibid.
[197] See supra note 99.
[198] Ibid., p. 1.
[199] Ibid.
[200] Ibid.
[201] Ibid., p. 8.
[202] Ibid., p. 7.
[203] See supra note 43, p. 5.

days and that his target for completing a personnel security investigation was less than 100 days.[204]

Also testifying regarding the length of time it takes to complete a security clearance investigation, Deputy Assistant Secretary of Defense J. William Leonard stated, "The reason why the arrow is pointing to the left[205] is because in one particular category, the most complex cases, OPM case completion times have gone up beyond the standard. However, the reason for that is because of the amount of work that we are giving out, we are dependent upon what I call 'third-party providers of information.' We have to do FBI checks, INS checks, State Department checks, what have you. Those are the other activities that we are dependent upon. The more we push out, the more they have to respond to. That is the challenge we have today as a community. I have directed my people to get together on a community-wide effort. We need to collectively address this, because it is not an OPM problem, it is a community problem that impacts DSS and impacts every other agency that does background investigations."[206]

5. Defense Security Service [DSS] and the Office of Personnel Management [OPM] personnel security clearance investigators have difficulty accessing State and local criminal history record information [CHRI].

The Personnel Security Investigations Process Review Team reported, "Conducting a local agency check to obtain a criminal history record is a national requirement for all security clearance investigations. In some cases, a criminal history record can be obtained from State and federal repositories, thus fulfilling the local agency check requirement. However, the cooperation and priorities of local law enforcement agencies providing criminal history records varies depending on jurisdiction. In many cases, conducting a local agency check can cause significant delays in closing a PSI investigation."[207]

"State and municipal law enforcement agencies do not receive separate funding or resources for conducting local agency checks and often require payment for such checks as local policies dictate. Payment of fees does not appear to be an effective inducement for local agencies to comply with requests in an expeditious manner as response time does not change as a result of payment."[208]

DSS drafted proposed legislation which required access be given by all States to criminal history information through automated systems where available. "The legislation passed without two key aspects: authorization for federal agencies to obtain criminal history record information on the basis of name or other common iden-

---

[204] Testimony of Lt. General Charles J. Cunningham, Jr., USAF (Ret), Director, Defense Security Service, NSVAIR Subcommittee hearing, Feb. 16, 2000, Serial No. 106–267, p. 88.

[205] Deputy Assistant Secretary Leonard is referring to a "Plan Success Factor" chart that compared success factors for processing PSIs by DSS and OPM. The success factor for OPM's Performance Expectations was pointing *left,* toward failure, even though overall OPM was at the high end of the chart. See NSVAIR Subcommittee hearing, Serial No. 107–40, p. 29.

[206] See supra note 139, p. 40.

[207] See supra note 37, p. 25.

[208] Ibid.

tifiers, and a prohibition on requiring indemnification agreements." [209]

The Personnel Security Investigations Process Review Team recommended the Office of the Secretary of Defense representative to the Security Policy Board [210] coordinate with the Department of Justice to develop incentives for local enforcement agencies to comply with requests for criminal history record information and to press for the enactment of the two unresolved issues.[211]

RECOMMENDATIONS

1. The Secretary of Defense should continue to report the personnel security investigations program including the adjudicative process as a material weakness under the Federal Managers' Financial Integrity Act to ensure needed oversight is provided to effectively manage and monitor the personnel security process from start to finish.

Given the fact personnel security investigations are not conducted in a timely manner; many investigations are not meeting required national investigative standards, and long range milestones are planned beyond fiscal year 2001 to improve DSSs automation capabilities, the subcommittee recommends DOD continue to report the Personnel Security Investigations Program as a material weakness under the Federal Manager's Financial Integrity Act [FMFIA].

The FMFIA requires DOD's senior managers to identify and solve department wide systemic problems. The General Accounting Office recommended this action as a result of their review of the PSI program. GAO found personnel security investigations were not conducted in a timely manner nor were they meeting Federal investigative standards, thus having a potential effect on national security. During the NSVAIR Subcommittee hearing in February 2000 Carol Schuster stated, "They are designating this investigation program, as a material weakness to the Department of Defense under the Federal Manager's Financial Integrity Act." [212]

The Department of Defense has made some headway in reducing the backlog of personnel security investigations as well as resolving the problems associated with tracking, processing, and adjudicating PSI's in a timely manner. However, the NSVAIR subcommittee recommends the Department of Defense continue to include the Personnel Security Investigation Program as a material weakness under the Federal Manager's Financial Integrity Act.

Specifically, the subcommittee recommends the Secretary of Defense include in the Annual Statement of Assurance what progress and what action the Defense Security Service and the Office of the Assistant Secretary of Defense (C3I) are taking with regard to achieving the September 30, 2002 target date for the elimination of the PSI backlog, and for reducing the time it takes to grant a security clearance for new PSI's and periodic reinvestigations.

---

[209] Ibid., p. 26.

[210] See supra note 16. [The Security Policy Board [SPB] was abolished pursuant to NSPD No. 1. The functions of the SPB were transferred to the National Security Council, Policy Coordinating Committee on Feb. 13, 2000.]

[211] See supra note 37, p. 26.

[212] See supra note 75, p. 22.

In a prepared statement submitted to the NSVAIR Subcommittee, the Deputy Inspector General stated, "We included the personnel clearance problem in the list of top DOD management challenges submitted to congressional leaders last December and recommend continued DOD and congressional oversight until the problem is truly resolved. I am confident that ultimately it is fixable with sustained management emphasis, but the current goal of eliminating the investigative backlogs by September 30, 2002, is clearly at risk. In addition, it is uncertain that all backlog cases will be adjudicated until well after that date." [213]

The DOD–OIG reported, "any large-scale shift of investigative workload back to DSS should be done incrementally and on a trial basis, with close oversight of the results. Any transfer must be justifiable on the basis that DSS will be able to out-perform OPM in terms of the cost, timeliness, and quality of investigations. The DOD–OIG plans additional audit work on these issues for the remainder of FY 2002." [214]

In addition, the Deputy Inspector General said, "I would not be surprised if the current plan has to be recast one more time, because I don't think that we can be fully confident that we understand how many new investigations are going to be required until the system (JPAS) that Mr. Money referred to, the new system (JPAS) that is just being fielded now, is actually in place and starts generating experience data that we can all rely on." [215]

Concerns regarding the viability of the September 30, 2002 target date were also raised by the General Accounting Office, "Then you've got the backlog cases, and then you've got the new cases coming in. So all told, we're talking about an enormous workload. I think they can submit the cases within the 2 years, but whether they can get them investigated and adjudicated, I have questions about that." [216]

2. The Secretary of Defense should set priorities and control the flow of personnel security investigation requests for all DOD components.

The Department of Defense does not have a centralized unit for tracking and prioritizing personnel security investigations and is therefore unable to determine the size or project an accurate date for the elimination of the PSI backlog. The NSVAIR Subcommittee recommends DOD establish a centralized unit to prioritize and control the flow of personnel security investigation requests.

According to DSS Director, General Cunningham, "The submission of requests for personnel security investigations is a function and responsibility of the individual military departments, defense agencies and defense contractors. More importantly, the Department of Defense prioritization comes from many sources and is difficult to integrate into our operations. This leaves the Defense Security Service at a severe disadvantage in trying to balance inves-

[213] See supra note 99, p. 19.
[214] See supra note 143, p. 3.
[215] See supra note 130, p. 37.
[216] See supra note 11, p. 46.

tigation requirements for a myriad of customers, all of whom have competing requirements and clearance needs." [217]

The General went on to say, "The personnel security process basically involves three phases, identifying the need for a security clearance and then prioritizing those requests, conducting the personnel security investigation, and adjudicating the PSI request." [218]

Regarding the issue of prioritization, the Acting Inspector General stated, "The April 2000 IG DOD report on Security Clearance Investigative Priorities [219] discussed a number of DSS case management issues. The principal concern was the lack of a meaningful process for prioritizing the workload. We determined that investigative resources were generally applied on a first in, first out basis, so that clearance requests for important programs and higher risk positions often languished while investigators worked on routine cases. Since timely investigations are a major problem, we deemed it particularly unreasonable not to have a viable prioritization process that both the requestors of the clearance and the investigators understand." [220]

The Assistant Secretary of Defense (C3I) Arthur L. Money stated, "There is a lack in CCMS to do prioritization. That is being fixed as another add-on to the software in April that will wash through the system, so by August there will not be this accumulation of cases, which have not worked their way through. So the prioritization will help the services once they prioritize." [221]

However, according to the Director of DSS, "With an anticipated significant number of security clearance requests expected through fiscal year 2001, it seems logical to me that the existing Department of Defense planning, programming and budgeting system would greatly improve the identification of requirements and simplify the process. It also seems logical that the establishment of central requirements facilities in the military departments would be most advantageous." [222]

The subcommittee also suggests the Office of Management and Budget [OMB] undertake a study to determine the feasibility of transferring the management of DOD's Personnel Security Investigation Program to the Office of Personnel Management and report their findings to the appropriate congressional oversight committees.

Legitimate concerns have been raised regarding the viability and the success of achieving the September 30, 2002 target for the elimination of the backlog. Deputy Assistant Secretary J. William Leonard stated, "The plan also extended the deadline for elimination of the investigation backlog until fiscal year 2002." [223] Deputy Assistant Secretary Leonard was referring to the directive issued by Under Secretary of Defense William J. Lynn's on June 22, 2000, "By using the services of the Office of Policy and Manage-

---

[217] See supra note 35, p. 80.
[218] Ibid., p. 81.
[219] See supra note 117, p. i.
[220] See supra note 158, p. 30–31.
[221] See supra note 122, p. 63.
[222] See supra note 35, p. 80–81.
[223] Testimony of J. William Leonard, Deputy Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, NSVAIR Subcommittee hearing, Serial No. 106–257, p. 55.

ment for select investigations, we plan to clear the backlog of clearances by fiscal year 2002." [224]

However, the Deputy Inspector General is skeptical DOD can achieve this target date stating, "The success of tracking, processing, and adjudicating PSI's in a timely manner is also doubtful. According to 2001 Defense Security Service data, it is taking 403 days on average for initial top-secret investigations, compared to 359 days in September 2000, when you had your last hearing on the subject. Likewise, it is taking 470 days on average for top-secret periodic reinvestigations, compared to 386 days in September 2000. The trends since this time last year have gone the wrong way, as far as this most sensitive part of the investigative workload is concerned." [225]

When compared to the results OPM is achieving, the Deputy Assistant Secretary J. William Leonard stated, "OPM's performance has been outstanding. They have—an earlier question from Mr. Kucinich in terms of how long it takes to do an investigation, they have established time lines, anywhere from 35 days for a background investigation all the way up to 180 days, depending upon what the requirements are. By and large, they are meeting those standards in every case." [226]

3. The Secretary of Defense should closely monitor the interface between JPAS and CCMS to ensure effective management of investigative and adjudicative cases and avoid further backlogs.

Without more consistent oversight of major information technology acquisitions, there can be no assurance that policy under the Clinger-Cohen Act is being translating into practice. Therefore, the subcommittee recommends the Secretary of Defense direct an immediate and one-time review of internal procedures to ensure compliance with the Clinger-Cohen Act by all DOD Military Departments and agencies, and the Office of Budget and Management initiate a review, cost/benefit analysis, and assessment of transferring the management and oversight of DOD agency information technology acquisitions to the General Services Administration [GSA].

The deficiencies in DOD's Personnel Security Investigations Program systems are in large part due to DOD's non-compliance with the Clinger-Cohen Act. Both the General Accounting Office and the Office of the Inspector General have raised concerns whether the CCMS and JPAS will be fully operational and integrated to accomplish the task of prioritizing, opening, tracking, and adjudicating personnel security investigations. Deputy Inspector General Robert J. Lieberman stated, "Unfortunately, the DOD historically has not has a strong record in the support systems area and the entire Defense Personnel Security Program clearly has been hampered by inadequate systems for many years." [227]

In regards to DOD's ability to eliminate the PSI backlog and prioritize PSI cases, the Deputy Inspector General said, "Everything is going to have to go right in terms of fielding new systems;

[224] See supra note 85.
[225] See supra note 99, p. 14–15.
[226] See supra note 139, p. 40.
[227] See supra note 99, p. 13.

and I know, Mr. Chairman, I have been over here on numerous subjects before you before, and the common theme running through all of them is that we have bad information systems and need something better, and historically, the track record for systems coming in on time, on schedule and actually being fully functional is not particularly good. So there is a risk there. If the new systems come in on schedule and are fully operational, we do not have anything that remotely looks like the CCMS fiasco, then we will have a fighting chance to get from here to there." [228]

The Department of Defense, Office of Inspector General released audit reports critical of DOD's acquisition management of both Case Control Management System [229] and the Joint Personnel Adjudication System.[230]

The DOD Inspector General reported, "Programs are defined as Major Information Technology Investment if OASD (C3I) determines that a program requires special OSD management attention because of the importance of the program's DOD mission, the high development, operating, or maintenance costs, or the program's significant role in administering DOD programs, finances, property, or resources." [231] "Despite, the system's (JPAS) criticality in support of DOD missions, acquisition management oversight was not provided in accordance with the Clinger-Cohen Act." [232]

CCMS and the Enterprise System for personnel security investigations were also allowed to proceed "without the benefit of program oversight and guidance." [233] "The failure of the Chief Information Officer (CIO) to actively participate in the acquisition of CCMS contributed greatly to the systems failures." [234] [235]

4. The National Security Council should promulgate Federal standards for investigating and adjudicating personnel security clearances in a timely manner.

Federal standards do not contain any specified time requirements for agencies to complete their investigative work for granting personnel security clearances. Because of the national security implications resulting from the length of time it takes agencies to grant security clearances, the subcommittee recommends that the appropriate National Security Council, Policy Coordinating Com-

---

[228] See supra note 130, p. 51–52.
[229] See supra note 28.
[230] See supra note 98.
[231] Ibid., p. 2.
[232] Ibid., p. 8.
[233] See supra note 28, p. 7.
[234] Ibid.
[235] The failure of OASD (C3I) to monitor and evaluate the performance of major IT systems appears to be a systemic problem that the subcommittee has found in other Defense Department agencies. [See *DOD Systems Modernization: Continued Investment in the Standard Procurement System Has Not been Justified,* (GAO–01–682), U.S. General Accounting Office, July 2001. NSVAIR Subcommittee hearing record, *The Standard Procurement System (SPS): Can the DOD Procurement Process be Standardized?,* Feb. 7, 2002, (in subcommittee files).] "The Clinger-Cohen Act of 1996, OMB guidance, DOD policy, and practices of leading organizations provide an effective framework for managing information technology investments, not just when a program is initiated, but continuously throughout the life of the program. Together, they provide for economically justifying proposed projects on the basis of reliable analyses of expected life-cycle costs, benefits, risks, and a basis for investment selection, control, and evaluation decision-making. The department has not met these investment management tenets for the Standard Procurement System." [See Statement of Joel C. Willemssen, Managing Director, Information Technology Issues, U.S. General Accounting Office, NSVAIR Subcommittee hearing record, p. 5, *The Standard Procurement System (SPS): Can the DOD Procurement Process be Standardized?,* Feb. 7, 2002, (in subcommittee files).]

mittee develop such Federal standards pursuant to National Security Presidential Directive No. 1.[236]

The General Accounting Office reported, "Defense Security Service customers (the military departments, DOD civilian agencies, and industrial contractors) and adjudication officials stated that they need DSS to complete its investigations within 90 days. The Office of Personnel Management uses a standard of completing its work in 35, 75, or a maximum of 120 days, depending on the price the customer is willing to pay for the service." [237]

According to Carol Schuster, "As I understand it, they are working to come up with some metrics that would have expectations for how long it should take for each kind of case. When we looked at investigations before, they were all over the board. So there isn't any standard right now for how long it should take for a particular kind of case. And there is any number of kinds of cases in this 2.2 million backlog. Some of them are very automated and don't take really very much time, and others are full field investigations that require a whole lot of work and over 200 days to complete." [238]

5. The Secretary of Defense and the Attorney General jointly should develop a system which allows DSS and OPM investigators access to State and local criminal history information records [CHIR].

During the March 2001 DSS oversight hearing, Assistant Secretary of Defense Arthur L. Money said in his prepared statement, "In closing, I would like to ask for your help. First, we need automated access to State and local government criminal history records akin to that provided law enforcement agencies." [239]

In that regard, Deputy Assistant Security J. William Leonard indicated DSS investigators could only access local and State criminal history record by means of a fingerprint card. Secretary Leonard stated, "We have to submit finger print cards, which is a time-consuming and expensive process. In those instances where we cannot access their automated records, we literally have to send an agent out, put shoe leather on the ground, go to the local police office or local sheriff's office and stand in line." [240]

Recently, subcommittee staff was advised by GAO that since September 11th there has be a greater demand for FBI fingerprint records for background checks by State and local officials. As a result, the increased demand for fingerprint cards is placing a greater burden on DSS to complete personnel security background investigations in a timely manner. The Department of Defense needs to develop policy in conjunction with the appropriate NSC Policy Committee to develop a system which will allow for better access to local and State criminal records by DSS agents and to submit Congress any legislation needed to implement this change.

○

[236] See supra note 16.
[237] See supra note 27, p. 16.
[238] See supra note 11, p. 45–46.
[239] Statement of Arthur L. Money, Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, NSVAIR Subcommittee hearing, Serial No. 107–40, p. 32.
[240] See supra note 139, p. 64.